Universidad
Carlos III de Madrid

Departamento de Informática

PROYECTO FIN DE CARRERA

AUDIT SYSTEMS:

APLICACIÓN DE AUDITORÍA

Autor: López García, Mª Isabel
Tutor: Ramos González, Miguel Ángel

---

25 febrero 2011

Título: AUDIT SYSTEMS
Autor: López García, Mª Isabel
Director: Ramos González, Miguel Ángel

EL TRIBUNAL

Presidente: _____

Vocal: _____

Secretario: _____

Realizado el acto de defensa y lectura del Proyecto Fin de Carrera el día __ de _____ de 20__ en Leganés, en la Escuela Politécnica Superior de la Universidad Carlos III de Madrid, acuerda otorgarle la CALIFICACIÓN de

VOCAL

SECRETARIO PRESIDENTE

Agradecimientos

Especialmente agradezco a D. Miguel Ángel Ramos, de Auditoría de Sistemas de Información y de Calidad del Software en la Universidad Carlos III de Madrid, la mayor parte de los conocimientos que actualmente tengo en esta materia. Afortunadamente fue uno de mis profesores y con él tuve la suerte de aprender temas de suma importancia, que me han valido mucho en mi vida profesional.

También quisiera darle las gracias por haberme aceptado bajo su tutela y haberme apoyado en el proceso de realización del proyecto, considerando que lo he desarrollado mientras trabajaba y que no ha resultado sencillo.

Por supuesto no quisiera dejar de agradecer a la universidad y a cada uno de los profesores que he tenido, las enseñanzas que me han aportado. Si bien realicé esta carrera por vocación, tras estudios previos y dejando a un lado el trabajo que en aquel entonces tenía, a fecha de hoy puedo asegurar que fue una decisión muy acertada y que sin duda, ha merecido la pena.

Resumen

De todos es bien sabido que tanto las auditorías informáticas, como los procesos de control de calidad del software, cada días son más valorados por todas las empresas, siendo además casi de obligado cumplimiento tanto en grandes compañías como en empresas que pretendan tener una certificación que las avale en el mercado, cada día más internacionalizado.

Estas empresas acuden a auditores externos e internos, que siguiendo una metodología determinada persiguen una mejora en los procesos de las empresas auditadas. Normalmente este proceso requiere de revisiones periódicas.

Se trata por tanto de un proceso laborioso que requiere el tener información precisa sobre la legislación vigente, de realizar recogida de datos en las empresas, de procesarla, de elaborar informes y recomendaciones que permitan mejorar los procesos, etc.

Existe por tanto una necesidad; existe de igual modo personal experto en la materia. Sin embargo a fecha de hoy no existen aplicaciones en el mercado que ayuden al auditor a realizar su trabajo, o bien éstas son demasiado simples para poder obtener un beneficio real que cubra las distintas partes del proceso.

Por tanto este proyecto nace de la necesidad por un lado de realizar estas auditorías y controles de calidad; y de la carencia por otro lado, de aplicaciones que den respuesta a estas necesidades.

Audit Systems es una aplicación que incluye una metodología basada en los Objetivos de Control (Control Objectives for Information and Related Technology) de ISACA. Su función es:

1. Administración de usuarios de la empresa.
2. Recogida de datos del personal en función del cargo que desempeñen.
3. Análisis y procesamiento de los datos recogidos conforme a la metodología que incorpora.
4. Realización del informe final a reportar a la dirección, incluyendo resúmenes de puntos a corregir y recomendaciones a tener en cuenta.

Audit Systems plantea preguntas de forma dirigida en función del cargo del encuestado. Los informes que genera son exportables y se pueden editar, dado que siempre se requiere que el informe final sea validado y aceptado por el auditor experto. Y su principal beneficio es que ahorra mucho tiempo de los auditores expertos, a la vez que sirve como registro del estado de los procesos de la empresa en cada instante temporal.

INDICE

1. INTRODUCCIÓN Y OBJETIVOS 10

1.1. INTRODUCCIÓN 10
1.2. OBJETIVOS 12
1.3. ÁMBITO DEL PROYECTO Y POSIBLES AMPLIACIONES 14
1.4. APORTACIONES PERSONALES 16
1.5. FASE DE DESARROLLO 18
1.6. MEDIOS EMPLEADOS 23
1.7. ESQUEMA DE LA MEMORIA 24

2. CUESTIONARIOS 25

2.1. INTRODUCCIÓN Y METODOLOGÍA 25
2.2. CUESTIONARIOS CON RESPUESTAS 25
2.3. CUESTIONARIOS VACÍOS 89
2.4. OTROS POSIBLES CUESTIONARIOS 113

3. AUDIT SYSTEMS 114

3.1. INTRODUCCIÓN. METODOLOGÍA APLICADA. 114
3.2. MÓDULO ADMINISTRADOR. 116
3.3. MÓDULO DE PROCESAMIENTO. 132
3.4. MÓDULO DE INFORMES. 141

4. CONCLUSIONES. 164

5. PRESUPUESTO 165

5.1. PLANIFICACIÓN DEL PROYECTO. 165
5.2. PRESUPUESTO POR PARTIDAS. 166
5.3. PRESUPUESTO DE VENTA MEDIANA EMPRESA. 167

6. GLOSARIO 168

7. REFERENCIAS 169

1. Introducción y objetivos

1.1. INTRODUCCIÓN

A lo largo de los siguientes capítulos el usuario-lector tendrá ocasión de informarse y aprender a usar la aplicación Audit Systems. Se trata de una aplicación de auditoría que incorpora la Metodología basada en los Objetivos de Control para la Información y Tecnología Relacionada de ISACA y que ha sido desarrollada con el fin de ofrecer apoyo al auditor experto en las labores base, las cuales toman mucho tiempo en los procesos de auditoría..

Recordemos que la Auditoría Informática es la rama de la informática que se encarga de la supervisión del control en entornos informáticos y plantea unos métodos y procedimientos de control de los Sistemas de Información que son válidos para cualquier empresa, independientemente de su tamaño.

Es indiscutible la creciente demanda de auditorías internas y externas por parte de las empresas. Habitualmente estas auditorías responden a cambios en entornos tecnológicos, económicos e industriales, que obligan a las empresas a adaptarse rápidamente a las nuevas circunstancias para poder sobrevivir y competir en el mercado; y como resultado de una cada vez mayor concienciación de que la información y la tecnología asociada a ella representan los activos más importantes de la empresa.

Por otro lado, la amplia gama de puntos abarcados por la Auditoría, nos acerca a un entendimiento global acerca del funcionamiento de la empresa: sistemas de información, tecnologías, equipos informáticos, grado de satisfacción de los usuarios, planificación, planteamiento de soluciones, estándares y metodologías, aspectos de control, de seguridad, etc.

La previsión, el control, la seguridad y la reducción de costes implicados en los Sistemas de Información, son una parte fundamental a tener en cuenta en las organizaciones. La automatización de las funciones y procesos, no obstante, genera una mayor dependencia de mecanismos de control en los ordenadores, que deberá ser supervisada en el proceso de auditoría.

De ahí la importancia cada vez más relevante de los procesos de auditoría, que ya se han normalizado en gran parte de las empresas y que ofrecen una garantía de calidad de los servicios ofertados en el mercado laboral. Es por ello que en la actualidad existe un gran número de empresas auditoras y departamentos de auditoría en las propias empresas. ¿Pero existen aplicaciones informáticas de auditoría que ayuden en la realización de este trabajo y que abarquen todos los procesos necesarios?

Lamentablemente no. Si bien los auditores se ayudan de las aplicaciones informáticas para la realización de su trabajo o parte del mismo, no es fácil encontrar aplicaciones informáticas desarrolladas expresamente para la realización del proceso de auditoría en empresas y menos aún si se pretende buscar una aplicación que abarque todos los procesos: recogida de datos, procesamiento, generación de

recomendaciones y elaboración de informes finales. Es por ello que no procede realizar una comparativa con otras aplicaciones de auditoría.

Por otro lado las auditorías son realizadas por auditores expertos en la materia que requieren de una formación continua en los marcos legales vigentes en cada momento y que están especializados en procesar y aplicar la información a cada empresa. Pero no se trata en absoluto de un proceso sencillo. Cualquier persona que intente profundizar en los marcos legales, que comience a navegar en las metodologías existentes y que empiece a plantearse de qué modo podría aplicar estas metodologías a las empresas cliente podrá entender la complejidad del proceso.

Resulta muy laborioso diseñar los pasos detallados a seguir para determinar si los procesos se están llevando a cabo de forma adecuada en la empresa. Del mismo modo es muy complicado plantear procesos de mejora, así como recomendaciones y procesos de seguimiento periódicos que sirvan para evaluar las mejoras y deficiencias de los procesos implantados en cada empresa. A continuación se verá que Audit Systems logra simplificar todos estos trabajos.

Cabe destacar que los informes finales generados por la aplicación ofrecen un valor muy importante a la dirección de la empresa. Estos informes ofrecen una visión simplificada de la adecuación en la ejecución de los procesos de la empresa y permiten a los empresarios tomar medidas rápidas y eficaces en base a las recomendaciones propuestas. ¿Y qué empresario no busca la eficiencia en los procesos y servicios de su empresa? Como bien es sabido por todos, la información es poder.

1.2. OBJETIVOS

A través de Audit Systems se ha procesado la información contenida en las metodologías y se han generado preguntas prácticas que recogen y evalúan el nivel de cumplimiento de los procesos de cada empresa, elaborando informes finales para reportar a la dirección de la empresa y a los responsables de auditoría.

Por tanto los objetivos que cumple Audit Systems son los siguientes:

1. Procesamiento de información contenida en las metodologías y elaboración de preguntas prácticas de recogida de información.

2. Administración de usuarios de las empresas cliente, asociando a cada perfil las preguntas que sean relevantes.

3. Recogida de información de los usuarios, evitando al auditor este proceso arduo y costoso en tiempo y reduciendo los desplazamientos necesarios.

4. Procesamiento de la información, comprobando las respuestas ofrecidas conforme a la metodología y detectando los procesos que no se están abordando de forma adecuada.

5. Generación de informes de forma automática. Se trata de informes inteligentes que constan de una introducción, de un desarrollo de información a través de distintos apartados y que incluyen resúmenes al final de cada capítulo sobre procesos que se deben corregir y sobre recomendaciones necesarias para la empresa auditada.

6. Procesos de exportación a distintos formatos, de tal modo que estos informes se puedan editar y sirvan de base al auditor experto para la incorporación de información y realización de los ajustes necesarios.

Como puede observarse la labor del auditor experto siempre será necesaria, tanto para la actualización de los cuestionarios de auditoría conforme a las nuevas leyes, como para la revisión del informe final y para la ampliación de información en los puntos que considere necesarios. Audit Systems por tanto ofrece los servicios que podría realizar un auditor menos experimentado, permitiendo de este modo al auditor experto profundizar mejor en los aspectos más importantes.

A continuación se muestra un esquema con las entradas y salidas que ofrece la aplicación:

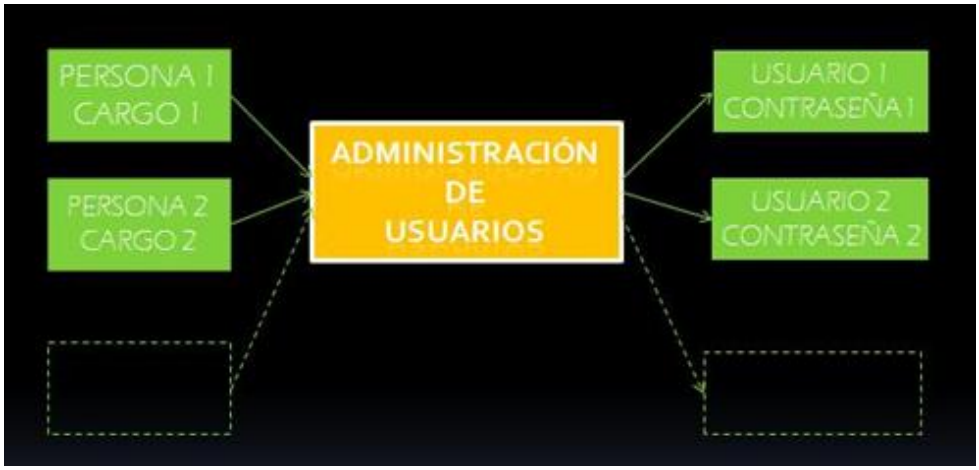


Figura 1. Entradas y salidas del módulo administrador

Figura 2. Entradas y salidas del módulo de procesamiento

1.3. ÁMBITO DEL PROYECTO Y POSIBLES AMPLIACIONES

El ámbito del proyecto es la realización de una aplicación generalizada, Audit Systems, que realmente sea útil al auditor experto en todos los procesos de trabajo que requiere la auditoría:

1. Recogida de información.
2. Procesamiento de datos.
3. Elaboración automática de correcciones y recomendaciones.
4. Elaboración del informe final exportable a otros formatos y editable.

Si bien se han contemplado todos los pasos necesarios, sería posible realizar futuras ampliaciones del proyecto. Éstas se relacionan a continuación:

- La aplicación consta de tres módulos principales: administración de usuarios, procesamiento de información y el módulo de informes. No obstante sería factible añadir a Audit Systems un cuarto módulo que le aportaría mucho más valor. Se trata del **módulo de gestión de cuestionarios**.

  Se trataría de un nuevo módulo accesible con la cuenta de administrador que permitiría visualizar, editar, crear y borrar tanto cuestionarios, como preguntas de los mismos.

  También debiese permitir la edición de la siguiente información:

  1. Información que se muestra en los informes de auditoría.
  2. Peso o importancia asignada a cada pregunta del cuestionario.
  3. Caja informativa con los pasos a seguir para corregir un proceso inadecuado.
  4. Caja informativa para casos en que sea necesario elaborar una recomendación.

- Sería también factible añadir un módulo adicional que realizase balance y comparativas de los resultados obtenidos en evaluaciones anteriores, con respecto a la nueva auditoría realizada en la misma empresa. Se trataría del **módulo de seguimiento**.

  Este módulo debiese constar de los siguientes puntos:

  1. Mecanismo de alarma y recordatorio mediante mensajes automáticos sobre puntos a solventar, en el plazo prefijado.
  2. Comparación automática de la nueva información con respecto a evaluaciones anteriores.
  3. Elaboración de informes de comparativa y seguimiento, que también incluyan sus recomendaciones y puntos a corregir.

- Llegando un poco más lejos y observando Audit Systems desde otra perspectiva, se trata de una aplicación capaz de evaluar, procesar y elaborar informes. Por tanto se podría diseñar un nuevo módulo que integrase otros tipos de cuestionarios, de tal forma que Audit Systems dejase de ser una aplicación de auditoría informática para **llegar a convertirse en cualquier tipo de aplicación de evaluación**, **aplicable a cualquier empresa**. Así por ejemplo para elaborar evaluaciones de exámenes, evaluaciones médicas, etc. Se trataría del **módulo de generalización**.

  Este módulo permitiría seleccionar el tipo de cuestionarios que se desee utilizar, que estuviera asociado al método de evaluación del mismo y también a las ventanas de recogida de información. El funcionamiento del resto de la aplicación continuaría siendo el mismo.

  Así por ejemplo Audit Systems tendría un modelo de cuestionarios basado en la estructura correcta, no correcta, no sabe no contesta, no aplicable. Internamente incorpora también la respuesta conveniente y las recomendaciones a seguir, información a partir de la cual genera los informes de salida.

  Para el caso de la evaluación de un examen de matemáticas se incorporaría un modelo más sencillo. Únicamente tendría dos entradas, una el resultado y la otra el desarrollo del problema. Internamente el procesamiento sería el mismo, realizando la verificación con respecto a la pregunta correcta, incorrecta y planteando las recomendaciones adecuadas. El auditor experto, que en este caso sería el profesor, reduciría considerablemente su trabajo. Una vez generados los informes realizaría las ediciones que considerase convenientes y el trabajo estaría finalizado.

  El nuevo ejemplo que considera una evaluación médica reutilizaría el modelo de cuestionario de la opción anterior. Así para un usuario concreto, que en este caso sería un paciente, se podrían introducir los resultados de un análisis. Internamente se realizarían las mismas comprobaciones internas para verificar si el resultado propuesto es acorde con el rango de valores que se considera saludable. Y nuevamente se reutilizarían los mismos informes donde se resumirían los puntos a mejorar, que en este caso serían tratamientos; y las recomendaciones a seguir.

  Como puede observarse este nuevo módulo y esta generalización ofrecerían un valor inestimable a la aplicación y que seguramente generaría muchos beneficios económicos.

1.4. APORTACIONES PERSONALES

Considero que la aportación más importante realizada a Audit Systems, es la **visión empresarial y práctica** que me han ofrecido los años de experiencia laboral.

De forma previa a la realización de la Ingeniería Técnica en Informática de Gestión, ya tuve la ocasión de trabajar con Cepsa interactuando con su Departamento de Calidad. Aún anteriormente tuve la suerte de trabajar en L'Entreprise Industrielle, de Dijon. En el departamento de calidad, donde yo trabajaba, se gestionaba un seguimiento de los distintos procesos, a través de la normativa propia de la empresa y de la ISO. Era necesario comprobar que los distintos procesos de control, implantados en cada fase, eran adecuados y se ejecutaban regularmente. También se tenía en cuenta el grado de satisfacción del cliente, reclamaciones, informes de control, etc.

Fue un trabajo muy enriquecedor que, entre otras cosas, me introdujo en el entorno de "La Calidad" y "La Auditoría" y me permitió tener un primer contacto con estos campos.

Estos conocimientos previos me han ayudado a tener una visión más amplia sobre el proceso completo de la auditoría y la calidad de la información en la empresa. También ayudaron a despertar en mí un mayor interés en todas las asignaturas relacionadas con este ámbito. De aquí se desprende que también realizase un Proyecto Dirigido relacionado con la rama de la auditoría, cuyo trabajo consistió en la elaboración de los distintos cuestionarios a partir de las normativas aplicables.

Además la aplicación Audit Systems ha sido desarrollada mientras trabajaba. Fue inevitable no evaluar los procesos internos y preguntarme a mí misma que pretendería de una aplicación capaz de realizar una auditoría informática.

El siguiente punto que más valoraría **es la simplicidad**. Personalmente siempre me gustaron los procesos sencillos y a partir de ellos poder alcanzar grandes retos. Este es uno de los puntos que he perseguido y que he logrado con este proyecto.

A continuación detallo este concepto:

- Los cuestionarios de recogida de información fueron evaluados de forma independiente.
- El módulo de administración fue diseñado y probado de forma independiente. Se validó.
- El módulo de procesamiento de información se generó de forma independiente. No era lo suficientemente generalizado. Sufrió unos cambios y se simplificó aún más. Se validó.
- El módulo de informes se realizó de forma independiente y tras ciertos ajustes también se validó.

Este proceso “divide y vencerás”, que permite de algún modo dividir en partes simples todo el trabajo, para posteriormente reunificarse en un todo, es lo que crea simplicidad en todo el trabajo.

También es esa misma simplicidad la que genera otro valor añadido: **la generalidad.** Como ya he comentado anteriormente resulta sencillo realizar formas complejas a partir de forma más simples. Pero no sólo eso, también da opción a ampliar la aplicación con futuros módulos que permitan dar respuesta a cualquier tipo de cuestionario relacionado con el ámbito de la auditoría. Y llegando un poco más lejos, ¿por qué no? Con nuevos módulos que permitan evaluar cualquier cosa, desde un examen hasta una evaluación médica. Así por ejemplo el mismo sistema sería válido para realizar diagnósticos en lugar de recomendaciones a partir de unos parámetros introducidos para cada usuario, que en este caso serían pacientes.

Todo el diseño de Audit Systems se ha realizado teniendo en cuenta la resolución de un problema general, en lugar de un problema particular. Así por ejemplo los distintos cuestionarios no han sido implementados a través de distintos formularios. La misma ventana es capaz de leer la información contenida en la base de datos mostrando en cada momento la pregunta que corresponda.

Lógicamente otra de las aportaciones personales realizadas ha sido la referente a los **conocimientos adquiridos en la Universidad Carlos III**, a través de las asignaturas impartidas (Auditoría Informática, Gestión de Calidad del Software, Ingeniería del Software, Bases de Datos, Sistemas de Seguridad, etc.)

De igual modo han ayudado distintas conferencias/cursos a los que he asistido sobre “Calidad” y sobre “Prevención de Riesgos Laborales”.

Cabe reseñar también como aportación personal **la detección de la necesidad del mercado** de una aplicación informática capaz de prestar servicio al auditor experto en la mayor parte de sus procesos, dado que actualmente no he logrado encontrar ninguna aplicación que los cubra.

1.5. FASE DE DESARROLLO

A lo largo de los siguientes puntos se detallan las fases del ciclo de vida en cascada que se han usado:

ANÁLISIS

Como ya se ha descrito anteriormente Audit Systems nace y responde a una necesidad existente. Por tanto su desarrollo nace en la fase de análisis del mercado.

En este análisis inicial se ha considerado la importancia de las auditorías y de la calidad del activo de la información. Se ha evaluado el incremento en la demanda de auditorías por parte de las empresas, tanto externas como internas.

Se han analizado distintos trabajos de auditoría, se ha **recogido información sobre las metodologías aplicables** y las leyes vigentes. Y en esta fase de análisis se ha buscado la forma de trasladar estas normativas a preguntas eficaces que sirvan al propósito de realizar la evaluación de forma generalizada de cualquier empresa.

En la fase de análisis se ha perseguido la **adecuación de preguntas conforme a los perfiles** que puedan tener los distintos usuarios. Se ha analizado de qué modo se realizaría el procesamiento de información, así como la elaboración y generación de los informes finales.

Para la generación automática de **informes** se realizó un **análisis previo** para que los párrafos generados fuesen acordes con los párrafos precedentes. Se tuvo en cuenta la **desaparición de espacios** en blanco cuando no fuese relevante mostrar información, así como la elaboración de puntos resúmenes y recomendaciones al final de los distintos capítulos, utilizando para ello mis conocimientos adquiridos en la ingeniería técnica informática y mi experiencia laboral.

Se analizó por tanto de forma generalizada la problemática a resolver y se realizó el diseño de forma conveniente para crear valor a cualquier empresa cliente.

Por último se adoptaron decisiones sobre las herramientas más adecuadas para la implementación.

DISEÑO

Todo este análisis previo se trasladó a un diseño del trabajo a realizar: parte gestora de administración de usuarios y parte funcional de elaboración de cuestionarios y recogida de información.

Una vez tomadas las decisiones precedentes, se comenzó a diseñar a más bajo nivel los pormenores necesarios:

- Diseño relacional de los distintos módulos, formularios y objetos.
- Distintas interfaces en función que se tratase de la parte de administración o de la parte de evaluación.
- Menús necesarios y barras de herramientas.
- Formularios a realizar, abstracción y comunicación entre las distintas capas.
- Funcionalidades a implementar, entradas y salidas.
- Diseño de base de datos, tablas y campos necesarios.
- Modelo relacional.
- Diseño y distintos prototipos de informes.
- Diseño de conectividad entre los distintos módulos.

La siguiente imagen muestra la conectividad existente entre los distintos formularios desarrollados en Visual Basic:

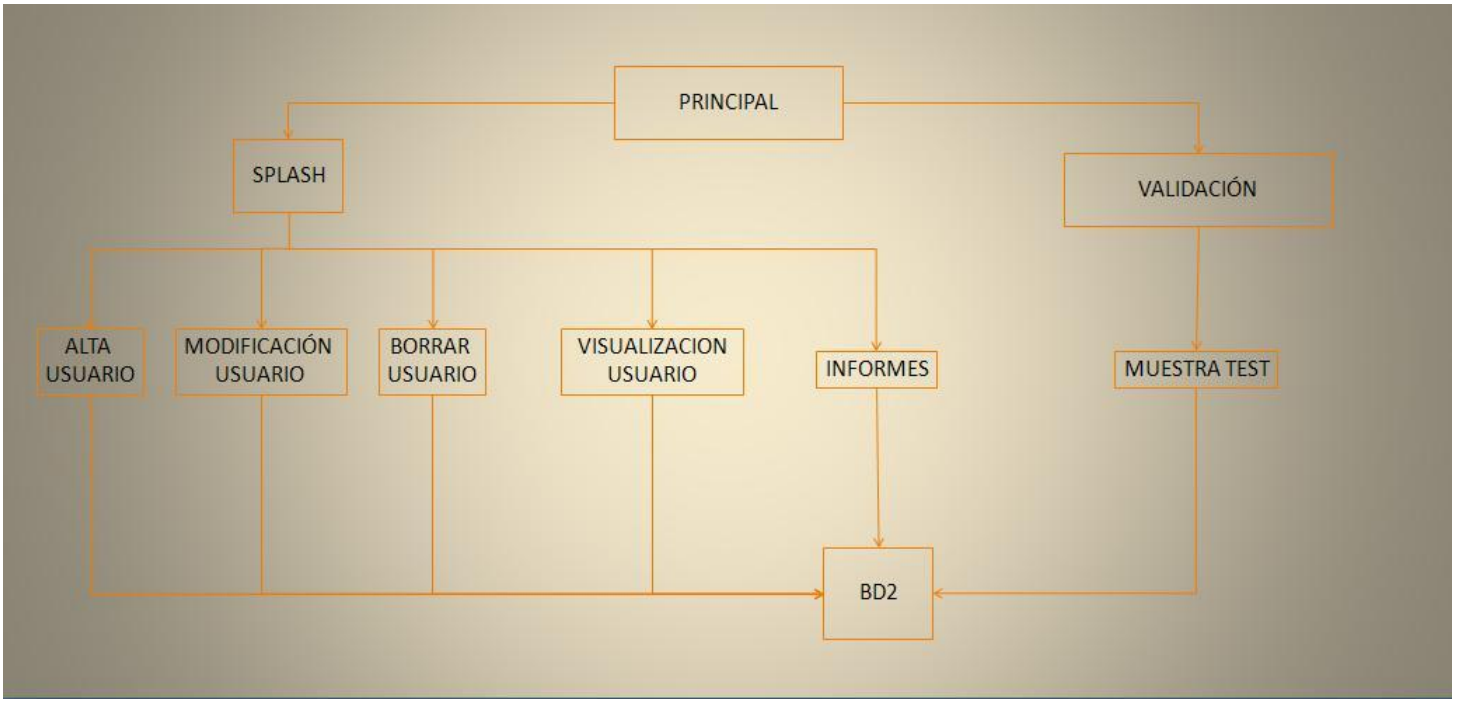


Figura 3. Relación interna de formularios desarrollados.

Al acceder a Audit Systems se accede al formulario principal que permite validar usuario y contraseñas de acceso y que permite entrar en el módulo administrador o en el módulo usuario.
Si se accede al módulo de usuario se puede acceder a los cuatro formularios de usuario en función de la operación a realizar: alta, modificación, borrado y visualización. También permite acceso al formulario de informes. Estos a un nivel inferior se comunican con el formulario de base de datos, que es el que realiza las comunicaciones con la base de datos.
Si se accede al módulo de informes, se valida el punto de inclusión de información para el usuario de acceso y permite acceder a los test-cuestionarios. A bajo nivel se comunica con el formulario que comunica con la base de datos.

Y a continuación un detalle de tablas y campos de cada una de ellas que se han diseñado en la base de datos:

FASES		
NUMFASE	FASE	DESCRIPCION
int	text	text

Figura 4. Tabla Fases.

FASETEST		
NUMFASE	FASE	TEST
int	Text	numeric

Figura 5. Tabla FaseTest.

PROFESION		
IDENTIFICADOR	CATEGORIA	PROFESION
numeric	text	text

Figura 6. Tabla Profesion.

TESTDIRECTOR	
NUMTEST	DESCRIPCION
numeric	text

Figura 7. Tabla TestDirector.

TESTOPCIONES					
TEST	OPCION	PREGUNTA	CRITICO	RESPUESTA	INCORRECTO
numeric	Numeric	text	bit	bityint	text

Figura 8. Tabla TestOpcione parte 1.

NSNC	CORRECTO	RESUMEN	RECOMENDACIÓN	RECNSNC
Text	Text	Text	Text	text

Figura 9. Tabla TestOpciones parte 2.

USUARIO					
IDENT	USUARIO	CATEGORIA	NIF	LETRANIF	NOMBRE
numeric	Text	text	text	text	text

Figura 10. Tabla Usuario parte 1.

APELLIDOS	DIRECCION	CPOSTAL	POBLACION	PROVINCIA	TELF	MOVIL	CARGO
text	Text	text	Text	text	text	text	text

Figura 11. Tabla Usuario parte 2.

USUARIOTEST		
USUARIO	TEST	ACABADO
numeric	numeric	bit

Figura 12. Tabla UsuarioTest.

USUATESTOPCION				
USUARIO	TEST	OPCION	CONTESTACION	COMENTARIOS
numeric	numeric	Numeric	numeric	text

Figura 13. Tabla UsuaTestOpcion.

VALUSUARIO			
IDENT	USUARIO	PASSWORD	CATEGORIA
numeric	text	text	text

Figura 14. Tabla ValUsuario.

DESARROLLO

A continuación se comenzó la fase de desarrollo de Audit Systems. Se construyó la base de datos necesaria y se fue implementando la aplicación utilizando una metodología de programación orientada a objetos, donde se buscó el encapsulamiento de la información, la abstracción de datos y un modelo relacional acertado.

Se construyeron las interfaces de recogida de información para los usuarios. Este proceso no fue satisfactorio y **fue necesario replantear el análisis y diseño** de esta parte, dado que inicialmente se pensó en realizar un formulario para cada cuestionario existente.

En el proceso de construcción se comprobó que no era el método más acertado, dado que requería de la implementación de multitud de cuestionarios con lo cual se trataba de un proceso muy laborioso y tedioso. Pero además no cumplía el objetivo principal que se estaba persiguiendo, que era la generalidad de la aplicación, su uso y su adecuación al mercado. ¿Qué ocurriría cuando cambiasen la metodología o las leyes existentes? ¿Sería necesario realizar nuevos desarrollos y nuevas interfaces de entrada con nuevas preguntas?

Es por ello que se adoptó entonces la decisión de dar marcha atrás, replantear el análisis y diseño de estas ventanas de recogida de información y en lugar de implementarlas a través de formularios, se adoptó la decisión de crear un formulario generalizado de preguntas que leyera automáticamente de la base de datos.

Este método de trabajo **permite** por tanto **actualizar la información de forma conveniente a lo largo del tiempo** de tal forma que genera un valor añadido para Audit Systems. A lo largo del tiempo no quedará desfasada y podrá seguir siendo útil en sus funciones.

El desarrollo de los **informes** tuvo cierta complejidad también. Para empezar se adoptó la decisión de priorizar la información que se mostraba en los informes mediante una ordenación automática en función de la criticidad de cada punto. Para ello se **asignaron distintos pesos** a las preguntas en función de los cuales la información se mostraría en un lugar o en otro.

Si bien el desarrollo fue sencillo conforme al diseño previo realizado, fue necesario realizar **múltiples ajustes y modificaciones** para conseguir que realmente de forma automática se generasen distintos capítulos, cada uno con sus recomendaciones y puntos que era necesario corregir.

Así por ejemplo en ocasiones no era necesario mostrar información, o no era necesario realizar recomendaciones. Era entonces necesario buscar la forma de hacer desaparecer esos espacios en blanco que no mostraban ningún tipo de información. No debe olvidarse que el objetivo final era presentar informes que pudiesen ser remitidos tanto a la dirección como al responsable auditor.

Se concluyó por tanto resolver el problema mediante partes modulares en los informes, programados de tal forma que **generasen de forma dinámica el informe principal** y que desapareciesen automáticamente cuando no debiesen mostrar información. Con todo ello el resultado tuvo éxito y se logró generar un informe adecuado para el objetivo que se perseguía.

Con respecto a la instalación de la aplicación comentar que permite instalaciones tanto en local como desde distintos puestos. En función de ello se deben adoptar las medidas de seguridad convenientes.

1.6. MEDIOS EMPLEADOS

A continuación se hace una descripción de los elementos que han sido necesarios para la elaboración de Audit Systems:

Hardware:

1. Ordenador portátil, Intel Pentium 1,60 Ghz, 2 Gb de RAM con sistema operativo Windows XP.

Software:

2. Paquete de Office 2007.

3. Microsoft Visual Studio 6.0.

4. Sistema Gestor de Base de Datos de Microsoft SQL Server. Microsoft Management Console 2.0 - Versión 5.1.

5. Crystal Reports 8.5.

Emplazamientos:

6. Biblioteca de la Universidad Carlos III de Madrid, a fin de consultar los libros relacionados en el apartado de referencias. En especial todos los relacionados con la auditoría informática y la calidad de la información.

7. Consulta en mi propia casa de los libros adquiridos mientras estudiaba distintas asignaturas de la Ingeniería Técnica en Informática de Gestión: Auditoría informática, Calidad del Software, Gestión de Proyectos, etc.

Otras fuentes de información:

8. Manuales de operativa de las aplicaciones: Visual Basic, Crystal Reports, a través de conocidos y documentación propia.

9. Internet y diversos foros informáticos para realización de consultas sobre acceso a la información, como por ejemplo conexiones a través de Orígenes de Datos ODBC.

10. Consulta a profesionales que trabajan como auditores, incluyendo casos en los que no pertenecían a la parte de auditoría informática, como por ejemplo auditores financieros.

11. Internet para búsqueda de información sobre la legislación aplicable en el ámbito de la auditoría, ISACA, COBIT, etc. Búsqueda de métodos prácticos para la realización de forma práctica del trabajo a realizar.

1.7. ESQUEMA DE LA MEMORIA

Capítulo 1 – Introducción al proyecto y planteamiento del problema. Exposición de la necesidad existente en el mercado y de los objetivos a cubrir, delimitando el ámbito que abarca. Introducción a las tecnologías en las que se centra el proyecto. Resumen de mis aportaciones. Enumeración de las fases de desarrollo, de los medios empleados, así como posibles ampliaciones del proyecto.

Capítulo 2 – Cuestionarios prácticos de evaluación empleados en el proceso de auditoría y que se utilizan para evaluar procesos en Audit Systems. Metodología aplicada.

Se divide en tres partes fundamentales: ejemplos de cuestionarios contestados y que muestran sugerencias de mejora, plantillas de cuestionarios elaborados sin contestar y posibles ampliaciones de cuestionarios que se podrían añadir.

Capítulo 3 – Aplicación Audit Systems desarrollada. Introducción. Sus módulos principales: administración, procesamiento e informes.

2. CUESTIONARIOS

2.1. INTRODUCCIÓN Y METODOLOGÍA

Audit Systems es una aplicación informática cuya labor principal es la de asistir al auditor experto a lo largo de todo el proceso de auditoría.

La fase de procesamiento de datos requiere de la realización previa e inclusión en la aplicación, de los cuestionarios que contengan las preguntas que se dirigirán al personal de la empresa, a fin de recoger la información necesaria para el proceso de auditoría.

Estos cuestionarios han sido realizados con una metodología basada en los Objetivos de Control para la Información y Tecnologías Relacionadas de ISACA, así como la Guía de Seguridad de SEDISI y se han cubierto los cuestionarios MARION. Se ha recogido información a través de las guías de buenas prácticas, se ha traducido información de algunos cuestionarios, algunas preguntas se han generado a partir de información de la ingeniería del software y los trabajos que se deben desarrollar, etc. Además se han elaborado también recomendaciones personales para los errores detectados, conforme a COBIT, guía de buenas prácticas, ITIL, experiencia laboral y errores comunes en las empresas.

A fin de mostrar un ejemplo sobre el uso de estos cuestionarios, posibles respuestas y posibles recomendaciones, esta sección estará dividida en tres partes: cuestionarios contestados, otros cuestionarios no contestados y posibles cuestionarios a desarrollar.

A su vez los cuestionarios han sido agrupados en función de la fase del proyecto a la cual pertenecen. Se ofrece la posibilidad de leer una breve introducción a cada una de las fases.

El esquema de cada pregunta es el siguiente:

Numeración – Pregunta – Si/No
Respuesta detallada

2.2. CUESTIONARIOS CON RESPUESTAS

- FASE DE ANÁLISIS

En la fase de análisis se plantea la resolución de un problema de negocio. Dependiendo del tipo de problema y sus posibles soluciones, se establecerá un proceso de desarrollo, de compra de paquetes integrados o reingeniería. Por tanto,

será necesario que el problema esté definido claramente así como adecuarse al ciclo de vida que más se ajuste al proceso. Será necesario que se especifiquen los procesos de datos, se recojan las necesidades del cliente y se aconseje acerca de las posibles alternativas de solución.

ANÁLISIS DE PROYECTOS – 1		
Nº	*PREGUNTAS*	RESPUESTAS
1	¿Se designan, o existen, grupos de personas encargadas de estudiar el problema, o el programa a desarrollar?	Si
Si, el equipo responsable del desarrollo se encarga de estudiar el problema a desarrollar.		
2	¿Existe un archivo o repositorio donde se registren proyectos finalizados así como los datos de su desarrollo?	No
No, de momento, aunque se tiene en mente realizarlo en un breve período de tiempo. Lo que sí se realizan son copias de los programas, o más bien de los distintos módulos, aunque no se guarda información relativa a su ensamblaje, uso, etc. Según los datos recogidos, una vez se realice dicho trabajo, desean tener la máxima seguridad en el archivo o repositorio, que posiblemente se trate de una caja fuerte y contenga los manuales y la metodología a seguir en la composición de módulos y librerías. En cuanto a los proyectos finalizados, estos sí se guardan, aunque sin la necesaria documentación de programa. Esto crea una fuerte dependencia de los programas desarrollados con respecto al director técnico, lo cual es altamente preocupante.		
3	¿Se consultan para estudiar problemas similares?	No
No se pueden consultar ya que no existe una documentación adecuada. No obstante, de momento existe un grupo reducido de personas en desarrollo y están especializados en el trabajo que desarrollan. Además, para cada empresa desarrollan soluciones a medida. Lo que sí existe es una fuerte comunicación entre los distintos desarrolladores, al tratarse de una empresa pequeña. Se detecta un grave problema si algunas de las personas, sobre todo los jefes de proyecto, deciden irse. Sobre todo aquellos más antiguos, ya que son los únicos que conocen el proyecto y cómo debe ser modificado. Dada la escasez de documentación, la falta de comentarios del código, la estructuración no normalizada (en proyectos antiguos) y la complejidad de los proyectos, se estaría abordando un grave problema, dado que a cualquier persona le llevaría mucho tiempo retomar el trabajo.		
4	¿Se estudian las consecuencias de implantar una metodología o un método?	No
No se hace un estudio sobre las consecuencias de implantar una metodología, pero sí se intenta realizar un producto a medida que cubra las necesidades del cliente, con lo que se presupone que siempre se derivarán unas consecuencias positivas.		
5	¿Hay documentos estandarizados en la empresa, para realizar la descripción de requisitos de un problema dado?	No
No.		
6	¿Se proponen distintas soluciones a cada proyecto?	Si
En cierta forma, ya que se busca la solución más óptima.		
7	¿Se documentan las distintas soluciones?	No
A veces ni siquiera se documenta la solución adoptada. En los nuevos proyectos, ya se está comenzando a documentar la solución adoptada, definiendo claramente los requisitos de usuario, dado problemas registrados anteriormente con algunos clientes, registrando documentos de análisis y diseño, etc. aunque se denota una escasez y falta de formalización de la documentación.		

8	¿Está establecida alguna metodología con el fin de seleccionar entre las posibles soluciones?	No
No se documentan las posibles soluciones. Directamente se intenta buscar la solución más adecuada.		
9	¿Las personas que estudian la adecuación de una metodología o ciclo de vida a elegir, cuentan con una larga experiencia en el desarrollo de este tipo de proyectos?	Si
Si. Las personas contratadas por la empresa cuentan con una gran experiencia y son profesionales cualificados. Siempre utilizan un ciclo de vida con prototipos, dado que se está considerando una empresa pequeña que desarrolla productos a medida y deben estar adaptados al cliente.		
10	¿Se realiza un estudio de costes/beneficios describiendo las características económicas de la solución propuesta?	Si
Si, se evalúan los costes / beneficios antes de la aceptación de un trabajo, pero no se documenta, ni se sigue una metodología para ello. Son los directores quienes deciden.		
11	¿Se realiza una descripción detallada de la solución recomendada, incluyendo la metodología a seguir?	No
No. No se cree necesario.		
12	¿Toda la documentación generada se archiva y guarda de forma adecuada y resulta de fácil acceso para el personal de la empresa con acceso autorizado?	No
No. La documentación generada (que normalmente no es la necesaria, ya que podría tratarse tan sólo del Manual de Usuario), es archivada y se guarda. Podría guardarse en los archivos personales del director técnico, en cuyo caso el resto de desarrolladores podrían pedírselo caso de necesitarlo, en el programa de desarrollo de código (distintos comentarios sobre los módulos), etc. En general hay escasez de documentación y no hay un lugar concreto donde registrar todos los proyectos de forma rápida.		

En consecuencia, se recomienda:

- Establecer una norma que obligue a hacer un estudio previo sobre la viabilidad del proyecto y del impacto que causará en la empresa cliente.

- Designar a un conjunto de personas expertas que se encarguen de estudiar y documentar las posibles soluciones a un problema dado, de tal manera que pueda verificarse que realmente se ha seleccionado la solución más acertada. Se recomienda la implantación de una metodología para abordar este punto.

- Generar toda la documentación necesaria y no sólo la que hay que entregar al cliente. Sería interesante crear un registro general de consulta al que todas las personas interesadas tuviesen acceso, donde pudiesen obtener información sobre documentación, módulos y proyectos que han sido generados y aceptados.

- Necesario comentar todo el código, hasta de proyectos antiguos. Se recomienda contratar a una persona en exclusiva para realizar este trabajo, para evitar posibles problemas caso de que un jefe de proyecto de un producto antiguo deje de prestar sus servicios en la empresa.

- Realizar una descripción detallada, tanto de la demanda del cliente como de la solución ofertada, así como de los plazos pactados, funcionalidades, etc.

- También se recomienda crear un repositorio que contenga documentos estándar y que resulte de fácil acceso al personal de la empresa. Debe contener la información conveniente para poder reutilizar información sobre partes de proyectos anteriores que sean de utilidad.

- Realizar un análisis de costes/beneficios en base a los parámetros que la empresa considere adecuados: tamaño y dificultad del proyecto, duración, tamaño de la empresa cliente o número de puestos clientes, servicios ofertados, etc. Se recomienda realizar un registro adecuado de los distintos análisis de costes, en un lugar al que sólo tengan acceso las personas autorizadas. De esa forma en el futuro, caso de expandirse la empresa, será posible que una persona pueda encargarse de preparar y controlar presupuestos en base a los datos registrados.

El trabajo de un auditor no se centra en estar de acuerdo con una solución propuesta para un proyecto, sino que deberá fijarse en la adecuación del proceso que produce esa solución.

ESTUDIO PREVIO II - 2		
Nº	*PREGUNTAS*	RESPUESTAS
1	¿Existe un proceso definido (y utilizado) que se utilice para encontrar una solución al problema propuesto?	No
No, normalmente son los propios desarrolladores, quienes cuentan con una gran experiencia, quienes se ocupan de encontrar la solución más acertada.		
2	¿Han sido definidas y documentadas las necesidades del usuario?	No
No. No se documentan, pero sí se evalúan mediante un estudio y una comunicación activa con el cliente. El cliente envía documentos y se establecen reuniones previas hasta formalizar el contrato. En anteriores contratos tampoco se introducían las funcionalidades demandadas por el cliente. Como se han registrado problemas en anteriores proyectos, ahora se está procurando definir en el contrato cuales son los requerimientos a los que se comprometen ambas partes.		
3	¿Están correctamente archivadas y firmadas por una persona responsable? (la aceptación, no-aceptación, motivos, etc.)	Si
Si. Normalmente se registran los contratos, pero no las propuestas de trabajo. Los contratos sí son firmados y archivados correctamente.		
4	¿Se ha desarrollado un estudio de costes/beneficios del proyecto?	Si
Si. El responsable, esto es, el director comercial, se ocupa de realizar un estudio de los costes / beneficios que supone el proyecto. También se encarga de ello el director técnico y en última instancia toman las decisiones conjuntamente. Normalmente no se documenta ni archiva.		
5	¿Existe alguna persona responsable de examinar este estudio y de evaluar si es, o no es razonable?	No
No. Normalmente existe una reunión formal entre los dos socios para realizar la aceptación o no-aceptación del trabajo.		
6	¿Existe alguna persona responsable de evaluar si con la solución propuesta se llegará a solventar el problema?	Sí
Si. Antes de aceptar el proyecto se hace un estudio de viabilidad y gracias a la experiencia del equipo se conoce si se va a solventar o no el problema. Si es necesario, o existen dudas, se mantienen reuniones con las personas adecuadas (por ejemplo con los propios desarrolladores) hasta tener una certeza absoluta de que, una vez aceptado el proyecto, se va a solucionar de la forma más adecuada.		
7	¿Los requerimientos de control del proyecto han sido especificados?	No
No. Se tiende a trabajar con prisas y sobre la marcha. Cada cual realiza un control sobre su propio trabajo.		

En consecuencia, se recomienda:

- Establecer metodologías a seguir a lo largo del ciclo de vida del proyecto, para cada una de las fases, así como planificar previamente los métodos de control necesarios.

- Definir las necesidades del usuario, en el propio contrato o en otro documento, estableciendo el grado de importancia de los requerimientos (imprescindible, importante o secundario). Se recomienda archivar este documento una vez sea firmado por la empresa cliente.

- Se recomienda realizar un estudio de costes / beneficios de cada uno de los proyectos realizados o propuestos y crear un registro que pueda ser accesible para las personas interesadas.

ASPECTOS DE CONTROL - 3		
Nº	*PREGUNTAS*	RESPUESTAS
1	¿Se establecen tolerancias (límites de aceptación) para los procesos a realizar? (Transacciones por hora, velocidad de transmisión, nº de plataformas de implantación...)	Si
Si. Realmente se establecen porque precisamente los proyectos que desarrollan tratan de optimizar los tiempos de respuesta buscando las soluciones más óptimas. Por tanto, a pesar de que no se defina la velocidad de transmisión o el tiempo disponible para realizar una transacción, queda definido indirectamente.		
2	¿Existen normas sobre autorizaciones definidas? (Para acceder a proyectos anteriores, para negociar con el cliente...)	No
No, porque no es necesario. Cada cual sabe cual es el proyecto que está abarcando, conoce sus competencias y responsabilidades. Todo el personal tiene acceso a los recursos de la empresa. El acceso a anteriores proyectos se realiza mediante petición justificada (no documentada) al director técnico.		
3	¿Existen métodos establecidos para asegurar la integridad de los ficheros que se manejarán a lo largo del proceso?	No
No. No se han establecido métodos. Tampoco se considera necesario ya que los desarrolladores saben cómo hacerlo. Señalan el peligro de perder mucho tiempo en temas burocráticos.		
4	¿Existe una política interna a seguir en cuanto a la ampliación de requisitos de usuario se refiere?	No
No		
5	¿Se comenta, negocia y registra en el contrato que se formaliza con el cliente?	No
No, no suele hacerse a no ser que el cliente lo solicite expresamente. No obstante una ampliación de requisitos constituye un nuevo trabajo y suelen realizarse ampliaciones cuando se demandan.		
6	¿Se estudia el impacto que podría tener en el proyecto un fallo del sistema?	Si
Si. Se conoce. Supondría una paralización del desarrollo.		
7	¿Existe un plan de contingencia definido para estos casos?	No
No, pero se piensa que sería posible encontrar soluciones alternativas.		
8	¿Se dispone de un centro alternativo donde poder seguir trabajando?	No
No, pero se piensa que sería posible disponer de un centro alternativo caso que fuese necesario.		
9	¿Previamente al desarrollo del proyecto se negocia con el cliente y se definen niveles de servicio? (Nivel de servicio para procesar una transacción, nivel de servicio para corregir un error de programación, nivel de servicio para instalar un cambio en la aplicación, nivel de servicio para responder a una petición del cliente...)	Si
Si, no se define exactamente el tiempo de procesamiento de una transacción, ni el tiempo que se tardará en dar un servicio, etc. pero en su caso se negocia con el cliente buscar una solución óptima y adaptada a su negocio y ofrecer el máximo nivel de servicio (atender las peticiones) en el mínimo tiempo posible (dependerá de los proyectos que se estén abordando en el momento y de si hay personal disponible).		

10	¿Se definen accesos a la aplicación? (Es necesario definir previamente los niveles de seguridad de los que deberá disponer la aplicación)	Si
Si. En las distintas reuniones con el cliente se definen los niveles de seguridad de los que deberá disponer la aplicación que se está realizando.		
11	¿Se establecen las relaciones que deben existir entre los recursos del sistema y el personal? (Quién puede acceder a qué recursos, con qué propósito y con qué permisos.)	No
No, en un principio todo el personal tiene acceso a los recursos que están disponibles. Para acceder a los recursos que no están disponibles (como puede ser proyectos finalizados), será necesario realizar la petición pertinente.		
12	¿Existe una metodología a seguir para calcular el coste estimado?	No
No, normalmente son los dos directores quienes se encargan de la aceptación / no-aceptación de las distintas propuestas. Siguen criterios razonables que no siempre son económicos, pero ninguna metodología.		
13	¿Y para añadir un beneficio?	No
No. Tampoco siguen una metodología. Hacen una estimación en base a sus conocimientos y experiencia.		
14	¿Se define la medida deseada por el cliente para implementar cada objetivo?	No
No. No se define. Sí se negocia de forma previa a la aceptación del trabajo cuáles son las necesidades del cliente y si será posible satisfacerlas.		
15	¿Están reflejados y documentados todos los objetivos que puedan satisfacer al cliente? (Puntos críticos, importantes y secundarios)	No
No, no se documentan.		
16	¿Se identifican estándares, políticas y procedimientos generales para el desarrollo de aplicaciones?	No
No. Normalmente trabajan en base a la experiencia en el desarrollo y al tratarse de un grupo pequeño de desarrolladores no suelen surgir problemas. Cuando surgen, los directores se encargan de solucionarlos.		
17	¿Resultan de fácil acceso y consulta para el equipo de trabajo?	No
No, ya que no hay.		
18	¿Se utilizan y tienen en cuenta para el desarrollo de un proyecto?	No
No, ya que no hay.		
19	En cuanto al material que se recibe en la oficina periódicamente (software, revistas informáticas, periódicos, etc.), ¿se determinan las personas que tienen acceso a estos recursos?	Si
Si ya que en un principio vienen dirigidas a nombre de la persona responsable. No obstante algunas veces las cogen otras personas antes, o las cogen porque la persona responsable no está, etc. En general todo el mundo tiene acceso a estos activos.		
19	¿Se establecen metodologías para controlar su entrada?	No

No. Quizás si algún mes no se recibiese una revista o los productos software no se detectaría, dado que no se controla la entrada y que además no se sabría si alguien los ha cogido o dónde están. En teoría todas las revistas que se reciben junto con el software que les acompaña, así como el software que se recibe de distintas compañías (Microsoft, ILOG, etc.) deberían estar archivados en los lugares habilitados para ellos. Por el momento se ha conseguido ordenar el software de forma correcta, ya que antes se encontraba sin archivar, metido en grandes cajas, lo cual hacía inviable buscar el software necesario. En cuanto a las revistas, simplemente desaparecen sin que el personal tenga ocasión de verlas.		
19	¿Se registra la entrada de estos activos en algún documento y se guardan de forma adecuada?	No
No, ni se controla ni se registra.		

En consecuencia, se recomienda:

- Establecer normas sobre autorizaciones: para acceder a material de la empresa, a software, para tratar con el cliente, etc.
- Establecer una metodología que asegure la integridad de los ficheros.
- Definir una política interna para tratar las peticiones de ampliación de requisitos.
- Establecer un plan de contingencia que sea seguro y fiable, capaz de actuar frente a un fallo del sistema y que contemple un centro alternativo, caso que fuese necesario.
- Establecer una metodología para el cálculo de costes.
- Establecer y documentar los requerimientos del cliente, señalando el grado de importancia de cada uno de ellos. También se recomienda archivarlo una vez haya sido firmado por el cliente, de tal forma que pueda ser consultado por personal autorizado.
- Establecer estándares, políticas y procedimientos generales para el desarrollo de aplicaciones, que resulten de fácil acceso para el personal de la empresa y establecer métodos de control para verificar que se cumplen.
- Determinar las personas responsables de controlar los recursos que se reciben en la empresa periódicamente, creando un registro de entrada y controlando las personas que las están usando en cada momento. Determinar procedimientos para notificar su ausencia y corregirla.

ESTABLECIMIENTO DE PUNTOS FINANCIEROS - 4		
Nº	*PREGUNTAS*	RESPUESTAS
1	¿Se identifican correctamente todos los puntos financieros relativos a un proyecto software? (Comprobar en documentación)	No
No se identifican todos los puntos financieros. Cierto es que se presenta un presupuesto de acuerdo a la decisión tomada por los dos directores, pero no se hace una estimación de los gastos que va a suponer el proyecto, los recursos que van a ser necesarios, los beneficios netos que se van a obtener, etc. No lo creen necesario ya que esta información la conocen en base a la experiencia con respecto a anteriores proyectos y realizan el presupuesto en base a esos conocimientos.		
2	¿Existe algún responsable que se ocupe de verificar que los datos financieros que se asocian al proyecto sean completos y fidedignos? (Examinar la documentación del sistema y buscar responsables económicos de distintos puntos abordables en el proyecto)	No
No existe ningún responsable de verificar los datos financieros. En todo caso, si es necesario u oportuno, son los mismos directores quienes se ocupan de ello.		
3	¿Se identifican todos los riesgos asociados al proyecto? (Examinar en documentación, contemplar si se establecen distintos métodos para abordar cada riesgo y si se identifican todos los riesgos posibles)	No
No se identifican los riesgos asociados al proyecto, al menos en cuanto a documentación se refiere. No se cree necesario y se cree que estos trámites burocráticos perjudicarían al proyecto debido al tiempo que consumen. No obstante, los directores tienen en cuenta algunos riesgos tales como la fiabilidad del cliente. Han tenido anteriores problemas relacionados con este punto.		
4	¿Cada responsable tiene requerimientos precisos acerca del programa económico a seguir en cada punto del proyecto?	Si
No se presenta ningún problema con respecto a este punto. Normalmente no existen problemas económicos en cuanto a adquisición de recursos necesarios para el proyecto se refiere. Si existe alguna duda o gasto extraordinario se procede a una reunión con los directores para evaluar si es o no es procedente.		
5	¿Se ha establecido un método para determinar la estimación de costes relativos al proyecto? (Confirmar con el usuario que se trata de una estimación realista)	No
No existe una metodología para tales efectos.		
6	¿Los procedimientos a seguir se establecen de tal forma que las distintas actividades puedan realizarse en el tiempo acordado? (Examinar el tiempo de las actividades).	No
Este es un problema existente, ya que a pesar de haber contratado a más personal siguen necesitando un mayor número de personal experto, lo cual les resulta difícil de encontrar. Por tanto, en la mayoría de las ocasiones se encuentran desbordados por el trabajo y el tiempo asignado a las actividades puede llegar a ser insuficiente.		
7	¿Hay normas establecidas en cuanto a preservar la integridad de los datos?	No

No existen normas establecidas para preservar la integridad de los datos. En su defecto, el personal se preocupa por hacerlo. No obstante, hago constar que sería posible que surgiesen problemas, sobre todo con respecto a las modificaciones de programas y cambios de versiones se refiere.

En consecuencia, se recomienda:

- Identificar y documentar todos los datos financieros relativos al proyecto, tanto de costes estimados, beneficios estimados, recursos, gastos y beneficios reales, etc., responsabilizando a una persona de que los datos sean fidedignos.

- Identificar todos los riesgos asociados al proyecto, a ser posible previamente e intentar tomar medidas preventivas para abordarlos. Se recomienda hacerlo en base al impacto que puedan causar en el proyecto y a la probabilidad de que ocurra el riesgo.

- Realizan siempre una planificación del proyecto, donde se hagan constar todas las actividades relativas al mismo, incluyendo reuniones, tiempo necesario para la realización de la documentación, tiempo necesario para la aceptación del trabajo y para la aceptación por parte del cliente, etc.

- Establecer normas precisas en cuanto a integridad de datos se refiere. Será necesario que se diseñen documentos estándar y se lleve a cabo un control de las modificaciones realizadas a los programas y de las distintas versiones. Esta información deberá estar disponible para las personas autorizadas.

NORMAS RELATIVAS A AUTORIZACIONES DEFINIDAS- 5		
Nº	*PREGUNTAS*	RESPUESTAS
1	¿Han sido identificadas todas las transacciones clave?	Si
No documentalmente, pero se conocen cuáles son las transacciones que se derivan de cada uno de los proyectos.		
2	¿Se han determinado normas para autorizar cada una de las transacciones clave? (Verificar que las normas de autorización cumplen las políticas y procedimientos globales de la organización)	No
No hay normas ya que en un principio todo el personal está autorizado a realizar las transacciones oportunas para la realización del proyecto, de acuerdo a las funciones que desarrolla cada persona.		
3	¿Las distintas personas del equipo tienen claro quién puede autorizar cada una de las transacciones posibles? (Verificar que los miembros del equipo han sido informados correctamente)	Si
En un principio cada cual tiene conocimiento acerca de sus competencias. Las transacciones que no sean comunes siempre serán autorizadas por los directores.		
4	¿Existen especificaciones que determinen que deba grabarse el nombre de la persona que realiza/autoriza una transacción? (Verificar en la documentación)	No
No existen tales especificaciones.		
5	¿Se han establecido normas que determinen qué personas están autorizadas a obtener recursos pertenecientes a la empresa y bajo qué condiciones?	No
No se han establecido. Se considera que sería necesario hacerlo, dado que todo el personal tiene acceso a todos los recursos software. Además, no se establecen normas sobre qué hacer con manuales y versiones desfasados, que en ocasiones podrían tirarse a la basura y ser utilizados por cualquier persona que los encuentre.		
6	¿Se controla la entrada y salida de recursos que efectúan las personas autorizadas?	No
No. Cualquier persona tiene acceso a los recursos y en muchas ocasiones se llevan software, manuales y aplicaciones a casa con el objetivo de trabajar con ellos. No se realiza ningún control, por lo que en ocasiones al buscar algún CD no se sabe dónde está (alguien lo cogió porque lo necesitaba para realizar la implantación en una empresa, lo dejó en un despacho y no volvió a colocarlo en su sitio, se dejó dentro de alguna máquina, lo está utilizando una persona que trabaja en horario distinto, etc.).		

En consecuencia, se recomienda:

- Definir normas sobre autorizaciones de acuerdo a la funcionalidad de cada una de las personas integrantes en el equipo y al cargo que ocupan.

- Tener un control sobre las transacciones que se realizan en la empresa, registrando el identificador de la persona que la realiza.

- Establecer una normativa acerca del uso de los recursos pertenecientes a la empresa. Esta normativa deberá tener en cuenta de qué forma tratar el material que se queda desfasado.

- Se deberá nombrar a una persona responsable de controlar los recursos, de tal forma que todo el material esté controlado y se conozca en todo momento quién está en posesión de cada recurso y durante qué periodo de tiempo. Se deberá tener un documento de control a tales efectos.

INTEGRIDAD EN LOS ARCHIVOS- 6		
Nº	*PREGUNTAS*	RESPUESTAS
1	¿Han sido identificados los principales archivos? Comprobarlo con el usuario.	Si
Si, en cada uno de los proyectos se identifican los principales archivos en cierto modo, ya que se trata de módulos que posteriormente se ensamblan.		
2	¿Se identifican los componentes de los datos de los principales ficheros? (Confirmar con el usuario)	Si
Dependiendo de cada proyecto.		
3	¿Se han identificado los principales campos de control? (Confirmar con el usuario)	Si
Se identifican los distintos campos de control.		
4	¿Existe algún método para asegurar la integridad de cada uno de los campos del fichero? (Ver si es razonable)	Si
Las personas encargadas del desarrollo se ocupan de asegurar la integridad de cada uno de los campos de los ficheros.		
5	En un sistema multiusuario, ¿hay un usuario que tenga asignada la responsabilidad acerca de la integridad de los datos? (Ver si es razonable que se le haya asignado a la persona dada)	No
No, ya que todas las personas son responsables de la integridad de los datos, dentro del marco de trabajo en que desempeñan sus funciones.		
6	¿Se han determinado métodos para mantener controles totales independientes sobre los campos principales? (Ver si son razonables)	Si
Si, una vez que los propios desarrolladores han realizado sus propias pruebas y han finalizado su trabajo, alguien se encarga de realizar pruebas independientes. No obstante, no existen mecanismos automatizados a tales efectos.		
7	¿Se han establecido tolerancias (grados esperados) de los controles de integridad de ficheros?	No
No se han establecido.		

En consecuencia, se recomienda:

- Designar a una persona como responsable de la integridad de los ficheros.
- Hacer registrar, documentalmente, las pruebas realizadas a los ficheros. Se recomienda que estas pruebas sean diseñadas previamente.

RECONSTRUCCIÓN DE REQUERIMIENTOS -7		
Nº	*PREGUNTAS*	RESPUESTAS
1	¿Se ha determinado un criterio para reconstruir procesos de transacciones? (Ver si es razonable el criterio adoptado para la reconstrucción de transacciones con el tipo de aplicación de usuario)	No
No existe un criterio ya que en cada uno de los desarrollos se ofrece un desarrollo a medida, por lo que los procesos varían.		
2	¿Se ha establecido un criterio para reconstruir archivos? (Verificar si es razonable hablando con el jefe de proyecto)	No
No, por la misma razón.		
3	¿La documentación de análisis es adecuada y resulta conforme a los estándares? (Verificar que es adecuada y es completa)	No
La documentación de análisis resulta adecuada para los desarrolladores, pero no sigue los criterios de una documentación estandarizada.		
4	¿Se han determinado criterios para reconstruir procesos desde un punto en que se mantenga la integridad de datos? (Confirmar si el proceso de reconstrucción es razonable. Consultarlo al Jefe de Operaciones)	Si
Utilizando las copias de los ficheros. En estos momentos se realizan copias diariamente, cosa que no se hacía cuando comenzó el proceso de la auditoría. De cualquier forma, sería conveniente automatizar este proceso y señalar a una persona responsable que siempre estuviese disponible para realizar esta tarea, ya que actualmente esta función la realiza el director técnico.		
5	¿Se han definido controles de aplicación para todas las transacciones? (Verificar que se han incluido en las especificaciones del sistema)	No
No existen controles de aplicación para todas las transacciones.		
6	¿Se ha especificado un período de tiempo para la reconstrucción de la información? (Comprobar que los períodos de tiempo son conformes a la política de la empresa)	No
No se ha especificado ningún período de tiempo ni tampoco está definido en la política de la empresa. A su vez, ésta no está registrada documentalmente.		

En consecuencia, se recomienda:

- Diseñar una documentación de análisis estandarizada que sea válida para el desarrollo de los distintos proyectos.
- Determinar criterios para la reconstrucción de procesos desde un punto en que se mantenga la integridad de los datos. Podría tratarse de copias especiales, o al menos realizando alguna anotación en los archivos donde se haga constar que en ese punto del desarrollo se han verificado la integridad de los datos.
- Definir documentalmente la política de la empresa, de tal forma que esté disponible y sirva de referencia a todo el personal de la empresa.

IMPACTO DE FALLOS EN EL SISTEMA DE LA EMPRESA QUE AUDITAMOS- 8		
Nº	*PREGUNTAS*	RESPUESTAS
1	¿Se han identificado las pérdidas que supone un fallo en la aplicación del sistema? (Examinar si la pérdida es razonable)	Si
No se han identificado documentalmente, pero se conoce que un fallo en la aplicación del sistema provocaría una paralización temporal del desarrollo, con lo que las pérdidas tendrían una gran magnitud, tanto a nivel económico, como de imagen de la empresa, etc.		
2	¿Estas pérdidas se han supuesto para diferentes intervalos de tiempo (fallo de la aplicación durante una hora, ocho horas, un día, una semana, etc.)? (Examinar si las pérdidas para cada intervalo de tiempo son razonables)	No
No se han supuesto para distintos intervalos de tiempo. No obstante se conoce que a mayor tiempo mayor repercusión tendrá en el trabajo que se esté desarrollando en esos momentos.		
3	En el caso en que se produzca un fallo de sistema, ¿se ha tomado una decisión sobre como recuperar las aplicaciones? (Confirmar si la decisión tomada es correcta)	Sí
Se hará a través de las copias de seguridad, si bien es cierto que pueda perderse el trabajo de un día.		
4	¿Se necesitan procedimientos para un procesamiento alternativo en el caso en que el sistema quede inoperativo? (Confirmar la necesidad con el usuario).	Si
Si sería conveniente y una vez llegado el caso creen posible poder disponer de un centro donde puedan seguir procesando (basándose en buenas relaciones que mantienen con otras compañías).		
5	Si se necesitan procedimientos alternativos, ¿han sido especificados los procedimientos de procesamiento alternativo? (Confirmar con el usuario si son razonables los procedimientos de procesamiento de datos alternativos)	No
Sí se necesitan procedimientos alternativos pero no han sido especificados. Llegado el momento los directores se ocuparían de ello.		

En consecuencia, se recomienda:

- Identificar documentalmente y mediante cálculos justificados la pérdida que supondría una paralización del sistema en distintos intervalos de tiempo.
- Definir procedimientos para un procesamiento alternativo, caso de producirse un fallo en el sistema. Se recomienda que se tenga absoluta certeza sobre la disponibilidad del centro alternativo cuando se necesite.

IMPACTO DE FALLOS EN EL SISTEMA DE LA EMPRESA CLIENTE DE LA QUE AUDITAMOS -9		
Nº	*PREGUNTAS*	RESPUESTAS
1	¿Se identifican las pérdidas que supone un fallo en la aplicación del sistema? (Examinar si la pérdida es razonable)	Si
Si, se suele tener en cuenta el impacto que puede provocar en la empresa cliente un fallo del producto que le estamos ofertando. En base a ello se podrán tomarse mayor número de medidas de seguridad y control.		
2	¿Estas pérdidas se han supuesto para diferentes intervalos de tiempo (fallo de la aplicación durante una hora, ocho horas, un día, una semana, etc.)? (Examinar si las pérdidas para cada intervalo de tiempo son razonables)	No
No se especifican con tanto nivel de detalle, pero por ejemplo, para el desarrollo de una aplicación de compraventa en bolsa, un fallo podría suponer una pérdida grandiosa. Por tanto depende de la actividad de la empresa y de la funcionalidad de la aplicación que se esté desarrollando.		
3	El sistema propuesto ante las pérdidas, ¿es tecnológicamente aplicable en la práctica? (Confirmar con fuentes independientes y examinar si son, o no son adecuados, el hardware y software recomendados)	??
Se procura que no haya pérdidas ni caídas del sistema. No existe una política definida a tales efectos.		
4	En el caso en que se produzca un fallo de sistema, ¿se ha tomado una decisión sobre como recuperar la aplicación? (Confirmar si la decisión tomada es correcta; comentarlo con el usuario del sistema)	Si
Normalmente dependerá de la importancia del fallo. Si se tratase de un fallo ligero o de falta de conocimiento sobre la aplicación, se podrá dar solución vía telefónica, vía e-mail, o incluso personalmente llamando a un técnico. Caso de tratarse de un fallo grave que implicase una recuperación de la aplicación, deberían ponerse en contacto con la empresa que está siendo auditada (que es la proveedora del producto) para que solucionase el fallo. Si hubiese sido una tercera empresa la que hubiese desarrollado el producto, ésta se encargará de solucionar el fallo.		
5	¿Se necesitan procedimientos para un procesamiento alternativo en el caso en que el sistema quede inoperativo? (Confirmar la necesidad con el usuario).	??
Dependerá de la actividad de la empresa, pero normalmente sí lo necesitarán. Por su parte son las empresas clientes quienes deben tener en cuenta este punto.		
6	Si se necesitan procedimientos alternativos, ¿han sido especificados los procedimientos de procesamiento alternativo? (Confirmar con el usuario si son razonables los procedimientos de procesamiento de datos alternativos)	??
Dependerá de cada empresa.		
7	Si ocurriese un fallo en el sistema, ¿se han definido procedimientos para comunicárselo al usuario? (Confirmar con el usuario si el procedimiento de notificación es razonable)	Si

Caso de ocurrir un fallo en el sistema siempre podrán ponerse en contacto con la empresa objetivo de esta auditoría, tanto telefónicamente (número de la empresa y de móvil), como mediante el correo electrónico, FAX, personalizándose, etc.

En consecuencia, se recomienda:

- Definir políticas claras de servicio a clientes, ante caídas y fallos del sistema.

NIVEL DE SERVICIO SOLICITADO-10		
Nº	*PREGUNTAS*	RESPUESTAS
1	¿Se han especificado tiempos de respuesta para cada transacción? (Confirmar con el usuario si son razonables y si se cumplen)	Si
Se procura ofrecer los mejores tiempos de respuesta, ya que se desarrollan soluciones a medida. No obstante no se definen los tiempos de respuesta para cada transacción, por ejemplo en milisegundos ya que no se considera necesario.		
2	¿Se ha establecido una programación indicando qué parte del sistema se ejecuta en qué momento? (Comprobar si hay capacidad de proceso suficiente para prestar estos niveles de servicio)	No
No se ejecuta esta programación. No se considera necesario dada la alta capacidad de que disponen los equipos actualmente.		
3	¿En los contratos realizados se refleja el soporte de mantenimiento para el hardware y el software? (Revisar las especificaciones del contrato y asegurarse de que se recogen puntos sobre el mantenimiento)	No
Normalmente no se hace a no ser que el cliente lo demande explícitamente. No obstante la empresa se esfuerza en ofrecer el mayor soporte de mantenimiento ya que esto favorece a la imagen de la empresa y al negocio. Sin embargo, en el caso en que se contraten servicios de terceras empresas para desarrollar una parte del sistema, se suele recoger un compromiso por parte de ésta para ofrecer el mantenimiento adecuado de la parte desarrollada.		
4	¿Se han establecido las tolerancias o niveles de procesamiento para cada parte del sistema? Ej. Que se obtenga un informe entre 2 y 3 horas. (Confirmar con el usuario que las tolerancias de cada nivel de servicio son correctas)	Si
Si, cuando el cliente necesita un nivel de procesamiento especial lo especifica en los requerimientos y reuniones previas. La empresa auditada lo tiene en cuenta y cumple con sus compromisos.		
5	Las operaciones del sistema, ¿pueden procesar los datos dentro de las tolerancias establecidas? (Confirmar con el Jefe de Operaciones si las tolerancias son razonables)	Si
Normalmente los clientes están satisfechos con las tolerancias ofertadas ya que se desarrollan soluciones óptimas a medida de cada empresa.		
6	Las prioridades establecidas para la aplicación, ¿han sido comparadas con otras aplicaciones? (Confirmar con un miembro de la dirección si las prioridades de la aplicación son razonables)	Si
Siempre son razonables, caso de aceptarse el trabajo, ya que la empresa se compromete a buscar la solución más óptima. No es necesario que se comparen las prioridades con las de otras aplicaciones ya que se presupone que serán distintas, dado que se buscan soluciones adaptadas a la empresa cliente.		
7	¿Se ha proyectado en el tiempo, por un período razonable, el volumen de datos a procesar? (Confirmar con el Jefe de Operaciones que habrá suficiente capacidad para atender los incrementos en los volúmenes de datos)	No

No se hace porque no se cree necesario, dada la alta capacidad de los equipos actualmente.

En consecuencia, se recomienda:

- Proyectar en el tiempo el volumen de datos a procesar, para tener certeza de que se van a seguir ofreciendo los mismos niveles de procesamiento en las transacciones y que no van a surgir problemas en el tiempo de respuesta, almacenamiento, etc.

ACCESO DEFINIDO -11		
Nº	*PREGUNTAS*	RESPUESTAS
1	¿Han sido identificados los recursos necesarios para desarrollar la aplicación? (Confirmar con el usuario que los recursos han sido completamente definidos)	Si
Si. Siempre se definen previamente los recursos necesarios.		
2	¿Han sido identificados los usuarios que tendrán acceso a estos recursos? (Confirmar con cada responsable de estos recursos si los usuarios estarán autorizados para utilizarlos)	Si
Si, normalmente todo el personal tiene acceso a los recursos de la empresa. No obstante existen recursos propios de los desarrolladores, de la secretaria, etc.		
3	¿Han sido identificadas las personas responsables de los recursos? (Confirmar con el Jefe de Usuarios que estas personas son ciertamente las responsables de los recursos)	No
No. No existe ninguna persona responsable de los recursos. Cada cual sabe cuáles son los recursos que necesita para desempeñar su trabajo y los utiliza. No suelen surgir problemas con respecto a este punto.		
4	¿Se han establecido perfiles que relacionen los recursos con los usuarios autorizados para acceder a ellos? (Examinar en qué medida es completo el perfil de usuario)	No
No se establecen perfiles que relacionen recursos y usuarios. No se cree necesario.		
5	¿Existe un procedimiento para establecer el perfil de usuario? (Confirmar con el Jefe de Operaciones que los procedimientos son aplicables)	No
No existe un procedimiento a tales efectos.		
6	¿Se ha identificado la importancia de cada recurso? Ej. Un procedimiento de clasificación de recursos de seguridad. (Confirmar con la persona responsable que las clasificaciones de seguridad son correctas)	No
No se identifican pero se tienen en cuenta. Así pues se hacen consideraciones especiales con las librerías ILOG, etc. Para acceder a estos recursos, al igual que a módulos de proyectos finalizados, será necesario realizar la petición explícita al director técnico.		
7	¿Se han establecido procedimientos para controlar accesos no permitidos? (Evaluar si son razonables y suficientes)	No
No se han establecido.		
8	¿Se ha establecido un proceso para penalizar un acceso no permitido? (Confirmar con el jefe si hay una intención de implantar procedimientos en contra de estos accesos)	No
No se ha establecido.		

En consecuencia, se recomienda:

- Definir los recursos a los que puede tener acceso cada persona, dependiendo de su cargo o de la funcionalidad que desempeñe.

- Designar a una persona responsable de los recursos, procurando que sea una persona apta para desempeñar esta función (que disponga del cargo adecuado, que normalmente esté en la empresa, etc.).

- Definir una norma que permita clasificar cada uno de los recursos existentes en la empresa y que exprese de qué manera deben tratarse (confidencialidad, acceso, etc.)

- Establecer procedimientos para controlar accesos no permitidos, así como políticas de penalización.

EFECTIVIDAD DE COSTE - 12		
Nº	*PREGUNTAS*	RESPUESTAS
1	El hardware y software, ¿se obtienen mediante una oferta competitiva? (Examinar si los procedimientos para conseguir la mejor oferta son razonables)	Si
Si, por ejemplo para la adquisición del hardware. Para la adquisición de software es diferente, ya que se buscan herramientas específicas necesarias para el desarrollo. De cualquier forma siempre se intenta conseguir una oferta competitiva, aunque no siempre sea posible.		
2	¿Existe en la organización un procedimiento relativo a la efectividad de costes? (Examinar el procedimiento)	No
No existe un procedimiento escrito a través del cual se establezca, por ejemplo, un número de ofertas a recibir, modos de buscarlas, que se deban archivar para poder consultarlas y verificar que se han pedido y comparado distintas ofertas. No obstante sí se comparan los costes en cuanto a material de oficina se refiere, reservas de viajes, compras de material informático, etc.		
3	La efectividad de costes para los proyectos software que se llevan a cabo, ¿siguen el procedimiento? (Examinar los cálculos y confirmar que han sido preparados de acuerdo a los procedimientos de la compañía)	No
No. En los proyectos software que se desarrollan no se tiene en cuenta la efectividad de costes, si no la calidad de los productos necesarios. De cualquier forma no se considera necesario, ya que los costes derivados de cualquier proyecto no suelen ser elevados, dado que se posee una suscripción con Microsoft para ir recibiendo mensualmente todos los nuevos productos necesarios para el desarrollo (por tanto este coste ya es conocido y asumido por la dirección). Otros grandes costes que se puedan tener en un proyecto son los derivados de la implantación del producto, sobre todo en los casos en los que hay que realizar grandes viajes (Emiratos Árabes, Israel, Francia, etc.). Este coste ya se considera en los contratos y en ocasiones se repercute a la empresa cliente.		
4	Las características de la aplicación que se está desarrollando, ¿puede variar de forma significativa el coste proyectado? (Confirmar con el usuario que no hay características adicionales que puedan causar una variación en el coste de manera significativa)	Si
Si, de hecho en muchas ocasiones existen variaciones que varían el coste del proyecto. No obstante se tienen en cuenta en la previsión y en el caso en que fuese necesario, se negociaría con el cliente. En los contratos ya se refleja que las demandas de nuevas funcionalidades deberán ser aceptadas y valoradas por la empresa, lo cual en algunos de los casos supondrá un coste adicional. Aunque debiera hacerlo, no siempre una nueva funcionalidad supone un coste adicional ya que los directores tienen en cuenta políticas estratégicas, como por ejemplo el valor de entrar en el nuevo mercado de un país.		
5	¿Existen características en la aplicación que puedan dar lugar a variaciones en los beneficios estimados de forma significativa? (Confirmar con el usuario que no existen tales características)	Si

Si existen tales características ya que siempre se puede solicitar una variación en el programa, demandar un mayor número de funcionalidades, etc. No obstante se tienen en cuenta y un cambio en las estimaciones daría lugar a una renegociación por ambas partes.		
6	La vida estimada para el proyecto a desarrollar, ¿es razonable? (Confirmar con el usuario)	Si
Si. Son los propios clientes quienes evalúan si es o no es razonable, pero en todos los casos suele ser razonable.		
7	¿Existe una planificación de la fase de diseño que identifique actividades, tareas, recursos (humanos y materiales) y costes? (Examinar en qué medida es completo el programa de trabajo desarrollado en la fase de diseño)	No
No se suele realizar una planificación designando tareas y asociándolas a personas y recursos ya que no se considera necesario y se cree que consumiría tiempo del proyecto. Normalmente los plazos de entrega son muy escasos, lo que acarrea un gran esfuerzo del equipo, trabajo de muchas horas extra no remuneradas en base a este concepto, etc. Esto también da lugar a que en muchas ocasiones no se haya generado toda la documentación necesaria y no se hayan realizado unas pruebas exhaustivas de los distintos módulos.		

En consecuencia, se recomienda:

- Establecer una metodología mediante la cual pueda verificarse que realmente se están consiguiendo las ofertas más competitivas, al menos en la adquisición de materiales donde se pretende que así sea.

- Realizar y archivar planificaciones relativas a todos los proyectos que se llevan a cabo, de tal manera que pueda asegurarse que se van a respetar los plazos acordados. Se recomienda asociar las actividades a las personas, a los recursos necesarios y a los costes estimados. También será necesario considerar las actividades relativas a la elaboración de documentación.

- También se recomienda hacer un seguimiento y ajuste de dicha planificación.

OBJETIVOS DE MEDIDA - 13		
Nº	*PREGUNTAS*	RESPUESTAS
1	Los datos requeridos por la aplicación, ¿se procesan con un nivel alto de fiabilidad? (Confirmar con las personas que generan datos)	Si
Si, siempre. Se tienen siempre en cuenta los campos que pueden ser nulos, la tipología de los datos, el manejo y modificación de los mismos, etc. En las operaciones multiusuario se tiene en cuenta el acceso a datos compartidos, las operaciones de Roll-Back, etc.		
2	¿Los datos necesarios para la comprensión del trabajo a realizar y para el desarrollo del proyecto son recogidos en el período de tiempo especificado? (Confirmar con las personas dedicadas a generar datos, si éstos son recogidos en el tiempo requerido)	Si
Si.		
3	Los requerimientos de usuario, ¿han sido definidos en un documento? (Confirmar con el usuario si son completos)	No
No, no se definen en un documento pero se definen a través de reuniones y un alto nivel de interacción con el cliente. En los nuevos proyectos ya sí se recogen todas las especificaciones funcionales y requerimientos de usuario en los documentos oportunos, tras las reuniones específicas.		
4	¿Los requerimientos se han establecido en términos métricos? (Examinar si el criterio para medir en qué medida son completos los requerimientos, es razonable)	No
No se establecen en términos métricos. En ocasiones se hace referencia al tiempo de ejecución, pero se hace en términos amplios (minutos) y se dice que depende siempre de la capacidad del sistema con que se esté ejecutando la aplicación, ya que normalmente la búsqueda de soluciones consumen toda la capacidad de memoria del procesador. En relación a ello decir que los clientes suelen comprar servidores con las capacidades recomendadas por la empresa cuando adquieren alguna aplicación.		
5	¿La solución del proyecto se ha elaborado conforme a los requerimientos de usuario? (Examinar las especificaciones del sistema y confirmar que satisfacen los objetivos de usuario)	Si
Si, la solución del proyecto siempre satisface los requerimientos del usuario. Además se van implementando nuevos módulos a medida en base a las demandas de los clientes.		
6	La lista de comprobación de datos, ¿puede ser desarrollada de tal forma que compruebe el cumplimiento de los objetivos? (Confirmar con las personas dedicadas al procesamiento de datos que los requerimientos se han recogido con suficiente detalle como para generar listas de comprobación de datos que los verifiquen)	No
No se suelen realizar listas de comprobación. En su defecto se trabaja teniendo claro cuáles son los objetivos a cumplir e incorporando al cliente en el proceso para que personalmente pueda comprobar el cumplimiento de los objetivos.		

7	¿Los procedimientos han sido especificados de tal forma que permitan evaluar el sistema implementado para asegurar el cumplimiento de los requerimientos?	Si
Si. Una vez implementado un módulo o funcionalidad del sistema primeramente lo prueban los desarrolladores, posteriormente el equipo de soporte finalmente el propio cliente procederá a evaluar la parte del producto para su aceptación, en base a los requerimientos establecidos.		

En consecuencia, se recomienda:

- Recoger en un documento los requerimientos de usuario de todos los proyectos, e incluso elaborar los de antiguos proyectos, con los niveles de aceptación para cada uno de los requerimientos (a ser posible métricamente) y el grado de importancia. Sería conveniente que el cliente firmase este documento de forma previa a la realización del trabajo y que se fuese indicando en un campo si ya ha sido implementado y aceptado.

- Añadir un documento-resumen que contenga las restricciones propias de cada entidad, dado que en estos momentos esta información la conocen solamente los jefes de proyecto que ya llevan tiempo trabajando con las empresas.

- Realizar listas de comprobación con datos reales, con el objetivo de que finalmente pueda verificarse si se han cumplido los requerimientos establecidos.

ESTÁNDARES, POLÍTICAS, PROCEDIMIENTOS Y REGULACIONES -14		
Nº	*PREGUNTAS*	RESPUESTAS
1	¿Se han identificado políticas y procedimientos aplicables a la organización? (Confirmar con las personas responsables de desarrollar políticas y procedimientos, que todas las políticas aplicables han sido identificadas)	No
No se identifican políticas y procedimientos aplicables a la organización, al menos documentalmente. Los directores poseen conocimientos acerca de políticas aplicables y son asesorados por personas expertas. No obstante las normas sobre cómo deben realizarse las cosas se ofrecen a nivel de palabra, sin crear documento alguno al respecto.		
2	¿Se han identificado estándares y procedimientos aplicables al procesamiento de datos? (Confirmar con el Jefe de Procesamiento de Datos si los estándares han sido identificados)	No
No se han identificados estándares y procedimientos aplicables al procesamiento de datos. No obstante este es un punto crítico en las aplicaciones que se ofertan y siempre se ofrece un nivel óptimo de procesamiento de datos.		
3	¿Han sido identificadas las regulaciones gubernamentales aplicables a la empresa? (Confirmar con la asesoría jurídica si las regulaciones aplicables han sido identificadas)	No
No. No han sido identificadas, al menos documentalmente. Sin embargo los directores tienen algunos conocimientos de regulaciones gubernamentales aplicables a través del asesoramiento de expertos. No obstante se piensa que deberían poner especial atención en algunos puntos, como pueda ser la Ley de Protección de Datos, dado que no existe una normativa interna a la empresa que regule la confidencialidad o forma de tratar los datos relativos a las empresas clientes. Tampoco se ha designado a un equipo perteneciente a la empresa que se ocupe de la seguridad de los empleados y de una posible evacuación, caso que fuese necesario. Tampoco se ha designado una empresa médica para atender a los empleados, etc. No se le da importancia a ninguno de estos puntos. Consultar anexos		
4	¿Se han identificado todos los procedimientos de control aplicables? (Confirmar con el departamento de control que todos los procedimientos aplicables relativos al control han sido identificados)	No
No se identifican procedimientos de control. En algunos proyectos se han comenzado a desarrollar planes de pruebas, que incluyen pruebas de compatibilidad de datos con versiones anteriores. En ocasiones se han tenido problemas a causa de este punto y casi ha supuesto la pérdida de un cliente.		
5	¿Se han identificado requerimientos aplicables al personal y la privacidad? (Confirmar con el departamento de personal si se han identificado todos los requerimientos aplicables al personal y la privacidad.	No

No se identifican documentalmente, si bien es cierto que en ocasiones tienen conocimientos sobre estos puntos. Por ejemplo sólo una persona tiene acceso a las nóminas. En otros puntos no está tan claro, dado que todo el mundo tiene acceso a todas las aplicaciones, passwords, permisos de administrador, etc.		
6	Todas las políticas aplicables, procedimientos y requerimientos, ¿pueden ser efectivos en el momento en que el sistema sea operacional? (Confirmar las fechas en que se implantaron políticas, procedimientos y regulaciones)	No
No. En lo que a mí respecta existe una carencia de políticas y procedimientos aplicables.		

En consecuencia, se recomienda:

- Identificar, elaborar y archivar políticas y procedimientos relativos a la organización. Será necesario que el personal de la empresa afectado tenga conocimiento sobre estas políticas y procedimientos generales y que estén expuestos en un lugar de al que todo el mundo tenga un fácil acceso.

- Identificar, elaborar y archivar estándares y procedimientos relativos al procesamiento de datos y a los sistemas de información. Será necesario que el personal de la empresa afectado tenga conocimiento sobre estos estándares y procedimientos.

- Identificar, conseguir y archivar regulaciones gubernamentales aplicables. Será necesario que el personal de la empresa afectado tenga conocimiento sobre estas regulaciones.

- Definir procedimientos de control para todos los proyectos y verificar que dichos procedimientos se cumplen. Esta información debe resultar accesible para las personas afectadas.

- Identificar, conseguir y archivar requerimientos aplicables al personal y a la privacidad de los datos. Será necesario que el personal de la empresa afectado tenga conocimiento sobre estas regulaciones.

- FASE DE DISEÑO

La fase de diseño implica una relación estrecha entre el usuario y el diseñador del sistema. En esta fase deberán convertirse los requerimientos definidos por el usuario en un proceso implementable en el ordenador. De esta fase podrán obtenerse distintas soluciones, por lo que será necesario que el diseñador y el usuario se mantengan en contacto (para escoger la solución que mejor se adapte a sus necesidades). En esta fase aún será posible realizar cambios a un bajo coste.

Normalmente en esta fase se producirán: especificaciones de entrada, de procesamiento, de archivos, de datos de entrada y salida, diagramas de flujo del sistema, requerimientos de hardware y software, especificaciones de procedimientos de operación manual, políticas de retención de datos de clientes, etc.

En esta fase, será preciso auditar los siguientes puntos: identificación de riesgos de la aplicación, determinar si los controles aplicados reducen los riesgos a un nivel aceptable, comprobar si la aplicación cumple las políticas, procedimientos, estándares y regulaciones, si la documentación del sistema es completa, si la aplicación resuelve el problema propuesto, etc.

El auditor deberá dirigirse hacia los siguientes aspectos:

- Controles sobre la integridad de los datos: La integridad de los datos comienza con la identificación de riesgos, seguida por decisiones tomadas por la dirección sobre como afrontar estos riesgos.

- Diseño de controles para la integridad de archivos: La integridad de ficheros se asegura con los métodos de identificación de fichero, controles automatizados de fichero, y controles independientes sobre cada fichero.

- Plan de contingencia: Proponer acciones ante problemas. Incluye métodos manuales para seguir trabajando cuando la aplicación automatizada ha quedado paralizada, procedimientos de respaldo (back-up) y de recuperación de datos, así como consideraciones relativas al sitio físico (Centro de Procesamiento Alternativo, Salas Vacías de Procesamiento Alternativo, acuerdos entre empresas).

- Método para alcanzar el nivel de servicio: En la fase de análisis se definió el nivel de servicio a seguir durante la ejecución de la aplicación. El método para conseguirlo se diseña en esta fase.

- Procedimientos de seguridad: El perfil de seguridad indica quien tiene acceso a qué recursos. Los procedimientos y herramientas, así como las técnicas necesarias para implementar esta seguridad deben ser diseñadas en esta fase.

- Efectividad de coste recalculada: Hay que ajustar la estimación realizada en la fase de análisis.

- Verificar los objetivos a conseguir con el diseño: Los objetivos establecidos en esta fase deben establecerse conforme al ciclo de vida propuesto.

- Diseño y métodos: Una vez identificados estándares, políticas, procedimientos y regulaciones, la fase de diseño determina cómo el sistema puede cumplir con esos requerimientos.

CONTROLES SOBRE LA INTEGRIDAD DE LOS DATOS - 15		
Nº	*PREGUNTAS*	RESPUESTAS
1	¿Se han establecido controles sobre la tipología de los datos y los valores que aceptan los campos?	Si
Se establecen los controles adecuados en los programas que se realizan.		
2	¿Se controlan las transacciones de entrada, como p.ej. nº secuenciales de entrada? (Revisar si los controles establecidos sobre las entradas son adecuados y aseguran que la entrada está completa)	Si
Si, se tienen en cuenta y se controlan que las entradas sean correctas. Normalmente se establecen automáticamente los números que deben ser secuenciales. No siempre se hizo así y existen programas antiguos que no controlan la secuencialidad de los datos, que no dan error en el momento de introducir los datos y que posteriormente no funcionan. Se intenta ir corrigiendo estos problemas.		
3	¿Se establecen controles sobre las comunicaciones para asegurar la correcta y completa transmisión de los datos? (Revisar si los controles son adecuados)	Si
Si, se establecen controles y en el caso en que haya errores en las comunicaciones existen medidas que notifican el error. Por ejemplo si no se envía un e-mail correctamente se recibirá un e-mail indicando que no se envió correctamente por tal causa. Al dejar software en el FTP se controla mediante llamada telefónica si han podido acceder a los datos sin problemas. En el envío de datos a través de mensajería se hace de forma personalizada, recogiendo los recibos de entrega.		
4	Para las transacciones en las que existe una clave de entrada, ¿se han preparado controles internos que las verifiquen? (Verificar si son adecuados)	Si
Si, existen controles para verificar las claves introducidas.		
5	Para las numeraciones en las transacciones de entrada, como pedidos de clientes, ¿se generan números internamente para asegurar que no se pierde ninguna entrada? (Verificar si los procedimientos para asignar números continuos son adecuados)	Si
Si, se generan números internamente y cierto es que ayuda a que no se pierda ninguna entrada.		
6	¿Se utilizan controles que comprueben los dígitos de un campo, como p.ej. un nº de producto, para asegurar que el nº de producto es adecuado? (Verificar que se han determinado restricciones que aseguran la correcta entrada de información)	Si
Si, se realizan controles sobre las entradas de datos, de tal manera que se impide la entrada de datos incorrectos.		
7	¿Se verifican las entradas de números, la secuencialidad de números generados y los totales, mediante programas de validación de datos para asegurar que las transacciones de entrada sean exactas y completas? (Verificar que los controles que se establecen al preparar las entradas manuales se implementan en programas)	Si

Si se hace, cuando es necesario. No obstante existen problemas en programas antiguos que no controlan bien algunos campos, pero según se detectan se van corrigiendo.

En consecuencia, se recomienda:

- Verificar la entrada de datos en todos los programas, realizando pruebas para corregir los errores existentes en los programas antiguos.

DISEÑO DEL MÉTODO DE AUTORIZACIÓN -16		
Nº	*PREGUNTAS*	RESPUESTAS
1	¿Se ha documentado un método para autorizar cada una de las transacciones? (Revisar la documentación para asegurar que las normas sobre autorizaciones están completas)	No
Documentalmente no consta ninguna metodología a seguir en cuanto a autorizaciones se refiere. Tampoco se cree necesario ya que al tratarse de una empresa pequeña siempre autorizan las transacciones los directores.		
2	Hay documentos cuya autorización es dependiente de la fuente que los origina (en contra de una firma), ¿puede esta fuente de origen ser verificada por la aplicación del sistema? (Determinar si las transacciones cuya entrada indica una autorización por sí misma, pueden sólo ser originadas por una fuente autorizada)	No
No hay documentos cuya autorización es dependiente de la fuente que los origina. Sí podría suponer una autorización un e-mail recibido por alguno de los directores, pero en tal caso la aplicación del sistema sí registra la persona que lo ha enviado a través de la dirección electrónica.		
3	En un sistema de múltiples usuarios, ¿la responsabilidad para acceder a módulos, códigos fuentes, FTP, etc. ha sido asignada a personas individuales? (Determinar si las responsabilidades de autorización han sido asignadas de forma adecuada)	No
No, en un principio todo el mundo tiene acceso a todas partes, partiendo de que todo el mundo posee la clave de administrador, con lo que ni siquiera quedaría registrado el usuario que ha accedido a cualquier parte.		
4	El método utilizado en las autorizaciones, ¿es consistente con el valor de los recursos que se autorizan? (Revisar si el método de autorizaciones es razonable en relación a los recursos que deben controlarse)	No
No ya que en un principio todo el personal puede acceder a los recursos que necesite, partiendo de la fuente del código de los proyectos sobre los cuales se esté trabajando, de un elevado valor. No tendrían acceso a recursos privados como el software de proyectos cerrados o información confidencial, que deberían pedir a los directores caso de necesitarlo.		
5	Si se usan claves de acceso, ¿existen procedimientos adecuados para proteger las claves de acceso (contraseñas)? (Revisar si los procedimientos para proteger las claves de acceso son adecuados)	No
No. Cualquier persona podría conocer la clave de correo electrónico de un compañero pidiéndosela a la empresa proveedora de servicios de internet, que se encarga de las cuentas de correo electrónico entre otras cosas. Las claves de los usuarios nunca caducan, no existen métodos sobre cómo establecerlas, existen equipos de trabajo sin clave de acceso, o con la clave de acceso general de administrador y de acceso a los servidores. La clave de acceso de un usuario se comparte con los compañeros para que puedan acceder al equipo, etc.		

6	Si se usan claves de acceso (contraseñas), ¿pueden ser cambiadas con una frecuencia de tiempo razonable? (Determinar si las frecuencias con que se cambian las claves de acceso son razonables.	No
No, existen equipos que tienen contraseñas que son inadecuadas, pero no las varían.		
7	¿Se han establecido procedimientos para informar a la dirección sobre transgresiones de autorización? (Examinar si el procedimiento para informar a la dirección sobre incumplimiento de autorizaciones es razonable)	Si
No existe un método definido, pero el procedimiento normal es hablarlo directamente con la directiva. Además resultaría muy difícil detectar cualquier problema, dado el bajo nivel de seguridad.		

En consecuencia, se recomienda:

- Documentar políticas, metodologías, procedimientos y todas aquellas normas que son necesarias para la entidad, partiendo por definir autorizaciones limitadas para los usuarios, claves unipersonales confidenciales con la estructura correcta, que sólo una persona conociese la clave del administrador, etc.

- Que sea necesario iniciar sesión como un usuario del sistema, cada uno con el propio, en todos los equipos. El sistema deberá ser capaz de registrar el usuario que haya realizado una acción importante (copia del código fuente, acceso a parte no autorizada, etc.). Dichas claves deberán cambiarse cada cierto período de tiempo, de acuerdo a un procedimiento que se establezca a tal efecto.

CONTROLES SOBRE LA INTEGRIDAD DE FICHEROS -17		
Nº	*PREGUNTAS*	RESPUESTAS
1	¿Se han identificado los campos de tal forma que sea posible verificar la integridad del fichero? (Confirmar con los usuarios que existen suficientes restricciones de integridad sobre el fichero basados en la importancia de los datos)	Si
Si, se identifican los campos y se verifica la integridad de los ficheros.		
2	¿Se han establecido procedimientos para verificar la integridad de los ficheros claves? (Examinar la documentación que indica la verificación aplicada para comprobar la integridad del fichero y determinar si es adecuada)	No
No existen procedimientos documentales para verificar la integridad de los ficheros. No obstante en la práctica sí se siguen procedimientos para verificar la integridad de los ficheros, esto es, pruebas por el equipo que desarrolla y pruebas posteriores por diferentes personas.		
3	¿Se han establecido procedimientos para informar a la dirección sobre variaciones en la integridad de ficheros? (Examinar las especificaciones y procedimientos para informar a la dirección sobre estas variaciones)	Sí
Si, ya que directamente se informa a la dirección o al jefe de proyecto.		
4	¿Se ejecutan con regularidad pruebas de control simples (total, más nuevos, menos borrados, igual a nuevo total) regularmente para asegurar que las modificaciones se ejecutan de manera apropiada? (Revisar si los métodos para asegurar que las actualizaciones se ejecutan de forma correcta, son adecuados)	Si
Si, en aquellas transacciones donde es necesario se ejecutan con regularidad.		

En consecuencia, se recomienda:

- Establecer procedimientos para informar a la dirección y para registrar en el documento de configuración y cambios, las variaciones realizadas a ficheros. Deberá registrarse la fecha en que se realiza, con qué finalidad, qué persona/s lo lleva a cabo, quién autoriza, dónde se registra la última versión, si se han vuelto a realizar pruebas de integridad, etc.

SEGUIMIENTO DE LA AUDITORÍA PROPIA DE LA EMPRESA -18		
Nº	*PREGUNTAS*	RESPUESTAS
1	¿Se han documentado especificaciones detalladas para cada objetivo de supervisión a realizar por la auditoría interna? (Por ejemplo, reconstrucción de transacciones individuales) (Revisar si la documentación está completa con relación a los objetivos de la auditoría)	No
No se han realizado especificaciones detalladas ya que nunca se le ha realizado una auditoría a la empresa, ni tampoco existe auditoría interna. Además esta auditoría tiene un carácter excepcional ya que ellos no la demandaron.		
2	¿Se han definido los campos y anotaciones necesarios para cada comprobación de auditoría? (Revisar los campos de datos para determinar si son razonables para satisfacer los objetivos de la auditoría)	No
a) No se definen campos ni anotaciones para la auditoría, ya que no tenían pretensión alguna de realizar ninguna auditoría.		
3	¿Se define el período de tiempo que se dedicará a cada seguimiento de auditoría? (Verificar que el período de tiempo dedicado es consistente con la política de retención de registros propia de la organización)	No
Tampoco definen el período de tiempo.		
4	¿Se han definido instrucciones para ser utilizadas en la auditoría? (Revisar si las especificaciones para formar a las personas en la puesta en marcha del proceso de auditoría, son completas)	No
No se han definido instrucciones.		
5	El recorrido de la auditoría, ¿incluye segmentos manuales y automáticos del sistema? (Revisar las especificaciones de supervisión de auditoría para verificar que tanto segmentos manuales como automáticos están incluidos)	No
No se ha definido ningún recorrido de auditoría.		
6	Los pasos de la auditoría, ¿se han definido en una secuencia y formato que hagan su uso sencillo? (Confirmar con los auditores internos si el formato y secuencia del recorrido de la auditoría es consistente con el uso que le dan en la práctica)	No
No existen auditorías realizadas. Esta es la primera.		
7	¿Se han establecido procedimientos para borrar los registros de programas de auditoría que han prescrito porque ya se les ha dado un uso completo? (Asegurarse de que los procedimientos de destrucción de estos registros de auditoría sean correctos)	No
No existen tales procedimientos, ni programas de auditoría.		

En consecuencia, se recomienda:

- Crear una función de auditoría de forma interna a la entidad.
- Realizar una auditoría externa, por su carácter independiente, anualmente.
- Documentar cuáles son los objetivos a cubrir por la auditoría y las especificaciones detalladas para cubrir cada objetivo.
- Definir los campos y anotaciones necesarios para las comprobaciones de auditoría.
- Definir el tiempo que se asignará a cada actividad de supervisión de la auditoría y a las actividades de seguimiento.
- Adquirir programas de auditoría que ayuden a realizar una supervisión de las actividades y transacciones realizadas.

DISEÑO DEL PLAN DE CONTINGENCIA -19		
Nº	*PREGUNTAS*	RESPUESTAS
1	¿Se han asignado responsabilidades para la preparación de un plan de contingencia? (Verificar que la persona asignada tiene suficientes aptitudes y tiempo para preparar el plan de contingencia)	No
No, no se han asignado responsabilidades, por lo que es responsabilidad directa de la directiva.		
2	¿El plan de contingencia define todas las posibles causas de fallos? (Confirmar con el Jefe de Operaciones que la lista de fallos potenciales está completa)	No
No existe un plan de contingencia.		
3	¿El plan de contingencia define responsabilidades durante el período de contingencia? (Revisar si la asignación de responsabilidades es completa y adecuada)	No
No existe un plan de contingencia.		
4	¿El plan de contingencia identifica recursos de contingencia? (Confirmar con el Jefe de Operaciones que los recursos asignados podrán estar disponibles en el periodo de contingencia)	No
No existe un plan de contingencia.		
5	¿El plan de contingencia determina las prioridades operacionales después de un problema? (Confirmar con un miembro de la dirección que las prioridades de recuperación son razonables).	No
No existe un plan de contingencia.		
6	¿Todas las partes involucradas en un fallo están incluidas en el desarrollo del plan de contingencia? (Revisar la lista de participantes en el plan de contingencia para comprobar si está completa)	No
No existe un plan de contingencia.		
7	¿Se han establecido procedimientos para comprobar la efectividad del plan de contingencia? (Revisar si los procedimientos de comprobación del plan de contingencia son adecuados)	No
No existe un plan de contingencia.		

En consecuencia, se recomienda:

- Realizar un plan de contingencia.
- Designar a una persona como responsable del plan de contingencia.
- Definir en el plan de contingencia todas las posibles causas de fallos.
- Definir responsabilidades durante el plan de contingencia.
- Determinar las prioridades durante y después del plan de contingencia.
- Comprobar la efectividad del plan de contingencia que se establezca.

MÉTODO PARA LLEVAR A CABO EL NIVEL DE SERVICIO DISEÑADO -20		
Nº	*PREGUNTAS*	RESPUESTAS
1	¿El sistema diseñado puede cumplir el nivel de servicio solicitado? (Confirmar si es razonable que se cumpla, hablando con el personal de operaciones, o bien ejecutar una simulación del sistema para verificar el nivel de servicio)	Si
Si, el sistema diseñado siempre cumple los niveles de servicio demandados, ya que se realizan desarrollos a medida y el equipo está especializado en dar el nivel de servicio que se ofrece.		
2	Un período de máximos volúmenes, ¿impactaría en el nivel de servicio deseado? (Desarrollar una simulación para comprobar si los niveles de servicio se basan en los volúmenes máximos procesados)	Si
A mayor volumen de datos se ralentiza la búsqueda de soluciones para los problemas planteados, pero siempre dentro de unos límites más que aceptables. A mayor volumen de datos los árboles de búsqueda para encontrar las soluciones más óptimas se elevan de forma exponencial. En los nuevos proyectos este dato se documenta y entrega al cliente. De cualquier forma nunca nadie se ha quejado ya que los tiempos que se ofrecen son valorados por todos los clientes.		
3	¿Podría ser que posibles errores impactaran en el nivel de servicio? (Determinar el número de errores que se prevén e incluirlos en la simulación del sistema)	Si
Podría ser, si existiesen errores graves. En ocasiones se han introducido datos incorrectos, bajo ciertas circunstancias y esto afectaba al nivel de servicio de la aplicación, no permitiendo la búsqueda de soluciones o haciéndolo de forma errónea. Ante un caso semejante los clientes llaman y el error es corregido.		
4	¿Se ha determinado el coste de no lograr el nivel de servicio deseado? (Confirmar con el usuario el coste de no lograrlo para comprobar que ha sido calculado)	Sí
Sobre todo perjudicaría a la imagen de la empresa. No afectaría al coste económico dado que el error sería corregido automáticamente.		
5	¿Los niveles de servicio deseados y proyectados vuelven a calcularse cuando cambia el sistema? (Examinar las peticiones de cambios en el sistema y determinar su impacto en el nivel de servicio)	Si
Sí, si cambia el sistema vuelve a evaluarse el nivel de servicio que se podrá ofertar, caso que incida en ello.		
6	¿Hay procedimientos establecidos para conseguir el nivel de servicio deseado? (Revisar si los procedimientos son adecuados)	No
No existen procedimientos establecidos, al menos documentalmente. No obstante el equipo es experto y siempre consigue el nivel de servicio deseado.		
7	¿Se pueden integrar suficientes recursos para conseguir mantener el nivel de servicio cuando los volúmenes aumentan? (Confirmar con el Jefe de Operaciones que los recursos del ordenador pueden aumentarse en orden al aumento en los volúmenes de datos)	Sí

Si, es posible aumentar la memoria del disco duro y la memoria RAM, conectar varios equipos, cambiar el servidor, etc.

En consecuencia, se recomienda:

- Hacer un registro con las peticiones de cambios por parte de los clientes, teniendo en cuenta de si se trata de una ampliación del sistema, demanda de mayor número de funcionalidades, etc. También sería conveniente registrar la fecha, las personas que llevan a cambio el cambio, registro de la última versión, modificaciones a la documentación, etc.

PROCEDIMIENTOS DE SEGURIDAD - 21		
Nº	*PREGUNTAS*	RESPUESTAS
1	¿Se han considerado técnicas de seguridad avanzadas como por ejemplo la criptografía? (Confirmar con la persona responsable de la seguridad de los datos que se han tomado medidas avanzadas de seguridad y se han implantado allí donde era necesario)	No
Se trabaja bajo TCP / IP, pero no se utiliza un cifrando como pueda ser el VPNs. De cualquier forma no se considera necesario cifrar los datos. Eso sí, nadie puede asegurar que el acceso a la red sea seguro (cortafuegos adecuado, detección de intrusiones, etc.).		
2	¿Se han evaluado las características del software (como por ejemplo de un sistema operativo) con propósito de seguridad y se han implementado características allí donde era necesario? (Confirmar con los programadores del sistema que se ha usado un proceso sistemático para evaluar las características del sistema software necesarias para la seguridad)	No
No, por ejemplo existen equipos que no tienen claves de acceso. Además el software de los equipos varía de forma considerable, dado que se actualizan los sistemas, las aplicaciones, se emulan entornos de clientes, etc.		
3	¿Se han diseñado procedimientos para proteger la emisión y el mantenimiento de claves de acceso (contraseñas)? (Confirmar con la persona responsable de la seguridad de los datos si los procedimientos de protección de claves de acceso son adecuados)	No
No, no existen procedimientos definidos. Algunos equipos no tienen clave de acceso y otros sí. No obstante las contraseñas no varían ni son adecuadas.		
4	¿Se han definido procedimientos para gestionar transgresiones de seguridad? (Revisar si la manera de gestionar las transgresiones de seguridad son adecuadas)	No
No, no existen procedimientos definidos. No obstante, de detectarse una trasgresión de seguridad se daría lugar a una reunión para solucionar el problema. Sería muy difícil detectar una trasgresión a la seguridad dado que todos los empleados tienen la clave de administrador, acceso a todos los equipos, etc.		
5	¿La dirección general tiene intención de tomar medidas (quizás acciones legales) contra las transgresiones de seguridad? (Confirmar con la dirección general su intención de tomar medidas en contra de las transgresiones de seguridad)	??
Llegado el caso y según la importancia del problema se evaluaría si es conveniente recurrir a acciones legales.		
6	¿Se han definido las necesidades de seguridad de cada recurso (aplicación, código, etc.)? (Revisar si la seguridad para cada recurso es adecuada y completa)	No
No se han definido documentalmente y considero que la seguridad para algunos recursos no es suficiente.		

7	¿Se ha asignado la responsabilidad de la seguridad de la aplicación a alguna persona? (Confirmar que dicha persona tiene suficientes cualidades y tiempo para ocuparse de la seguridad de la aplicación)	No
No, ninguna persona es responsable de la seguridad de la aplicación. En cuanto a las aplicaciones que se desarrollan, cada persona es responsable del trabajo que realiza. Los jefes de proyecto suelen guardar copias en la red, pero no está claro que se creen las copias de seguridad necesarias.		
8	¿El sistema está diseñado de tal forma que protege los datos privados? (Confirmar con el usuario si el diseño es capaz de proteger los datos más delicados o privados)	No
No, el sistema no protege los datos. En un principio todo el personal tiene acceso a los recursos y archivos que se encuentran en la red.		

En consecuencia, se recomienda:

- Evaluar y tener certeza absoluta sobre la seguridad de la red.
- Evaluar las características del software utilizado. Se recomienda que al menos se requieran claves de acceso en todos los ordenadores y que existan políticas para cambiarlas cada cierto período de tiempo. Sólo una persona deberá tener los permisos de administrador.
- Además se recomienda elaborar procedimientos y formar al personal en materia de seguridad, de tal forma que todos sean conscientes de su importancia. Deberán conocer acerca del tipo de claves que se pueden elegir, cómo actuar ante incidentes extraordinarios, etc.
- Sería conveniente designar a una persona responsable de seguridad, que tenga el perfil adecuado para desempeñar esta función, que disponga del tiempo necesario y que se encargue de supervisar que se llevan a cabo los procedimientos de seguridad que se establezcan.
- Definir procedimientos claros y precisos que indiquen cómo actuar ante transgresiones de seguridad.
- Definir documentalmente las necesidades de seguridad de cada recurso y actuar en consecuencia.

EFECTIVIDAD DE COSTE RECALCULADA - 22		
Nº	*PREGUNTAS*	RESPUESTAS
1	¿Ha sido recalculado el coste de desarrollo del sistema en base a su diseño? (Confirmar con el diseñador del sistema si el nuevo coste de sistema es razonable)	No
No, el coste del sistema no vuelve a recalcularse en base a su diseño. Se mantiene la oferta inicial. Pueden hacerlo así gracias a su gran experiencia en anteriores proyectos.		
2	¿Han sido recalculados los beneficios del sistema en base a su diseño? (Confirmar con el usuario si los beneficios son razonables.)	No
No, no se recalculan los beneficios ni se calcularon inicialmente. Los directores estiman los beneficios en base a su experiencia en anteriores proyectos.		
3	¿Ha sido recalculada la vida útil del sistema en base a su diseño? (Confirmar con el usuario si la expectativa de vida de la aplicación es razonable)	No
No, no se calcula la vida útil del sistema. En un principio la vida del software es ilimitado dado que se van implementando nuevas funcionalidades.		
4	¿Ha sido recalculada la efectividad de coste del nuevo sistema? (Confirmar con los contables de la empresa que el cálculo es correcto)	No
No, se hace un presupuesto de acuerdo al trabajo que hay que desarrollar y se tienen en cuenta todos los aspectos necesarios: recursos a utilizar, tiempo de desarrollo, etc. Para ello se reúne todo el equipo. Finalmente los directores realizan un presupuesto. Posteriormente nadie recalcula la efectividad de coste del sistema.		
5	¿Los cálculos de efectividad de costes garantizan la continuidad del sistema? (Confirmar con la dirección que el diseño del sistema es aún eficiente en términos de costes)	Si
Si, los cálculos realizados para elaborar el presupuesto siempre garantizan la continuidad del sistema, dado que nuevas funcionalidades llevan asociados nuevos costes.		

En consecuencia, se recomienda:

- Desarrollar un procedimiento a seguir para el cálculo de costes de un proyecto. Se recomienda que tanto los costes, como los beneficios previstos, como el resto de parámetros queden registrados documentalmente. Posteriormente se aconseja añadir a la documentación los datos reales, de tal forma que exista un registro de tipos de proyectos, parámetros estimados y parámetros reales.

VERIFICAR LOS OBJETIVOS DE DISEÑO A ALCANZAR -23		
Nº	*PREGUNTAS*	RESPUESTAS
1	¿Ha hecho el grupo de diseño cambios en la aplicación del sistema sin la aprobación del usuario? (Examinar los cambios introducidos así como todas las peticiones de cambio del programa para verificar que han sido aprobadas por el usuario)	No
No, el grupo de diseño nunca realiza cambios sin la aprobación previa del usuario.		
2	¿Hay un procedimiento de petición de cambio formal que deba seguirse para hacer todos los cambios en el sistema? (Examinar la adecuación y cumplimiento del procedimiento de cambios de programa)	No
No, no existe un procedimiento formal. Normalmente se recurre a llamar telefónicamente y concertar una entrevista, o a solicitar el cambio en las reuniones regulares, etc.		
3	¿Los objetivos del sistema son reevaluados y cambiados en base a cada petición de cambio aprobada? (Determinar los efectos que tienen los cambios de sistema aprobados, en los objetivos y determinar si los objetivos han sido cambiados de acuerdo a estos cambios)	No
Normalmente los cambios no implican una variación de los objetivos. No obstante, si así fuera, se abordaría el cambio de la misma forma, ya que sería el cliente quien solicita el cambio y lo que se persigue es la conformidad del cliente.		
4	¿El usuario reevalúa continuamente los objetivos de la aplicación del sistema en vista a como cambian las condiciones de negocio? (Confirmar con el usuario que los objetivos son cambiados según las variaciones en las condiciones de negocio)	??
Dependerá de cada tipo de usuario. No obstante los objetivos sólo son cambiados por petición del usuario. Por su parte, en la empresa intentan asesorar en lo máximo posible al usuario, informándole sobre los aspectos que puedan ser más adecuados para su negocio, de la integración con los sistemas informáticos implantados en la empresa, etc.		
5	¿Hay usuarios profundamente involucrados en el diseño de la aplicación del sistema? (Confirmar con el personal de procesamiento de datos del proyecto si existe ese tipo de usuario)	Si
Si, el cliente siempre está fuertemente involucrado en el proceso de desarrollo del producto.		
6	Si la alta dirección del usuario cambia, ¿la nueva dirección confirma los objetivos del sistema? (Confirmar con la dirección que los antiguos objetivos son los deseados)	Si
Si, normalmente no suelen existir problemas al respecto, ya que la decisión de adquirir un producto no depende exclusivamente de una persona, si no que la suele adoptar el comité de la empresa cliente. Además los contratos se firman, con el consiguiente compromiso de la empresa cliente.		
7	Si los objetivos se cambian, ¿se cambia en concordancia la forma de medir esos objetivos? (Examinar los nuevos objetivos para determinar que sus criterios de medición son razonables)	Si

Si, si los objetivos de la aplicación que se desarrolla varían, eso implica un gran cambio. Por tanto conduciría a la evaluación de la aplicación como si de una nueva aplicación se tratase, midiendo todos los aspectos necesarios y partiendo de cero si fuese necesario.		
8	¿Son auditables las especificaciones de diseño? (Verificar que lo son)	No
No, dado que no existe un procedimiento de diseño estandarizado en la empresa, ni se realiza auditoría alguna.		

En consecuencia, se recomienda:

- Elaborar un procedimiento formal de petición de cambios. Deberán reflejarse la fecha de petición de cambio, persona que demanda el cambio, cuál es el motivo que genera el cambio, quienes son las personas responsables de evaluar si el cambio es procedente, quién y cuándo se aprueba el cambio caso de ser procedente, etc.

- Establecer un procedimiento formal para la realización del diseño de cada aplicación.

MÉTODOS PARA LOGRAR CONFORMIDAD CON EL DISEÑO - 24		
Nº	*PREGUNTAS*	RESPUESTAS
1	¿Han sido determinadas las especificaciones de conformidad? (Confirmar con la parte responsable que estas especificaciones sean correctas)	Si
Si, se determinan las especificaciones de conformidad aunque no se registran en un documento. En los nuevos proyectos se recogen los requisitos de usuario, documento que va variando hasta que la empresa cliente da su conformidad a las especificaciones. Sólo se establecen los puntos importantes (por ejemplo, no se dice nada sobre el aspecto de la interfaz).		
2	¿La parte responsable ha especificado el nivel deseado de conformidad? (Confirmar con las partes involucradas que el nivel de conformidad requerido es correcto)	Si
Si, el cliente siempre especifica los niveles deseados para la aceptación del producto, dado que siempre solicitan los puntos importantes y no los secundarios.		
3	¿Se pueden comprobar los estándares, regulaciones, etc., durante la implementación, para determinar si cambian los requerimientos? (Confirmar con las partes involucradas que pueden comprobar el área que les concierne)	Si
En ocasiones varía la normativa vigente y se varían también ciertas especificaciones del proyecto.		
4	¿Han sido determinados los costes de conformidad de forma que puedan ser medidos en función de beneficios, sanciones, etc.? (Revisar con las partes involucradas los costes / beneficios de conformidad)	Si
Si, cuando el cliente está conforme se procede normalmente. Sin embargo, si el cliente no está conforme esto implica mayor tiempo de desarrollo para solventar el problema, no poder dedicarse a otros proyectos, perjudica la imagen de la empresa, etc. No se establecen sanciones económicas para los posibles incumplimientos de plazo.		
5	¿Se han establecido procedimientos para comprobar la conformidad a las especificaciones? (Revisar la adecuación de los métodos especificados de comprobación de la conformidad)	Si
a) Si, primeramente se realiza el desarrollo en base a las especificaciones recogidas de los clientes. Se hace un estudio de la necesidad del mismo, visitando la empresa cliente, para estudiar las compatibilidades con el software instalado. Los desarrolladores realizan las pruebas pertinentes. Caso de haber tiempo suficiente, el equipo de pruebas también lo hará. Por último el mismo cliente aprueba la parte implementada dando su conformidad o demandando pequeños cambios.		
6	¿Han sido especificados métodos para controlar la conformidad cuando el sistema llegue a ser operacional? (Revisar la adecuación de los procedimientos especificados para asegurar la conformidad durante las operaciones)	Si

Si, antes de que el sistema llegue a ser operacional, se procederá a la aceptación de la empresa y a la aceptación por parte del cliente. Además el cliente y la empresa están en estrecho contacto a lo largo del desarrollo del producto. Posteriormente, cuando el producto se instala en la empresa cliente, si es necesario se imparten jornadas de cursos para formar al cliente. Si éste no estuviese conforme con algún aspecto informaría a la empresa y se buscaría la solución más adecuada, variando una funcionalidad, implementando una nueva, etc.		
7	¿Se ha elegido una persona para establecer la conformidad con los requerimientos? (Verificar que la persona asignada tiene el perfil adecuado y dispone del tiempo necesario para cumplir con su responsabilidad)	Si
Los jefes de proyecto, subdirector, o director técnico en su caso.		
8	La documentación diseñada, ¿es adecuada y conforme con los estándares? (Verificar en qué medida es completa y adecuada la documentación diseñada)	No
No, no existen estándares de documentación en la empresa.		

En consecuencia, se recomienda:

- Registrar en un documento firmado por el cliente las especificaciones de conformidad en todos los proyectos.
- Establecer estándares para el diseño de aplicaciones. Verificar que se trabaja conforme a estos estándares.

- FASE DE PROGRAMACIÓN

La complejidad del desarrollo en la fase de programación dependerá en gran medida del trabajo realizado en la fase de diseño. Si las especificaciones se han definido y si han sido valoradas en correspondencia a alguna métrica de cumplimiento de requerimientos, simplificarán en gran medida las tareas de programación.

El auditor deberá corroborar que los controles y requerimientos definidos, se implementen de igual forma a como fueron especificados en la fase anterior. Además deberá revisarse la estructuración del código, así como la reutilización de instrucciones de código (por ejemplo en procedimientos de entrada y salida de datos, en procedimientos de validación de datos, etc.).

Los entregables que espera encontrar el auditor, como salida de esta fase, son:

- Especificaciones del programa.
- Programa ejecutable.
- Documentación del programa.
- Instrucciones de operación.
- Programa de procesamiento de datos y resultados de las listas de comprobación aplicadas al sistema.

La participación del auditor en esta fase se determinará en función de los resultados obtenidos en la fase de diseño. Cuanto más estime el auditor que los controles que se han producido como salida de la fase de diseño son adecuados, menor será el grado en que se involucre en esta fase.

Revisar el código que se está generando, no es la mejor tarea que pueda realizar un auditor, ya que a lo largo de esta fase la aplicación que se desarrolla estará sometida a cambios diarios. Los objetivos que debería considerar el auditor durante esta fase, son los siguientes:

- ¿Se está construyendo un sistema teniendo en cuenta su mantenimiento futuro?
- ¿Las especificaciones del sistema están siendo implementadas de forma correcta?
- ¿Los programas cumplen con los estándares de procesamiento de datos?
- ¿Se realizan suficientes pruebas al programa ejecutable?
- ¿El programa ejecutable está documentado adecuadamente?

Los puntos que debe revisar la auditoría durante la fase de programación son:

- La implementación de controles sobre la integridad de los datos: Los controles deberán implementarse de tal forma que logren alcanzar el nivel establecido de control de tolerancia.

- La implementación de métodos de autorización: Deben implementarse normas de tal forma que se dificulte el no cumplimiento de las reglas. Por ejemplo, si se establece una autorización con un límite, no se deberá permitir al personal que introduzca una cantidad que supere ese límite.

- Implementar controles de integridad de ficheros: La implementación debe minimizar la probabilidad de pérdida de la integridad de los ficheros. Los controles podrán ser preventivos, ante la pérdida de integridad de ficheros, o de detección, informando en un breve plazo de tiempo que se puede producir una pérdida de integridad.

- Implementación de programas de auditoría: Se debe implementar de tal forma que facilite la utilización de la información obtenida. Si el trabajo de auditoría contiene la información necesaria, pero es muy costoso usarla y supone mucho tiempo, el valor del programa de auditoría disminuye significativamente.

- Que exista un plan de contingencia escrito: Es la única manera de asegurar que las tareas planificadas se seguirán desarrollando en el caso en que existan problemas. Se debe asegurar que los datos y los recursos estarán disponibles cuando deba llevarse a cabo el plan de contingencia.

- Implementación de procedimientos de nivel de servicio: El nivel de servicio deseado tan sólo se plasmará en la realidad cuando los procedimientos y métodos están enfocados hacia el nivel de servicio demandado. Se deben realizar pruebas sobre el nivel de servicio para asegurar que cumple las especificaciones.

- Implementación de procedimientos de seguridad: En este punto se tendrán en cuenta la implementación de herramientas y técnicas de seguridad, así como el conocimiento y entrenamiento de los empleados con respecto a la seguridad.

- Efectividad de coste reevaluado: Según se implementa el sistema, frecuentemente los objetivos van cambiando. El cambio en los objetivos y el método de implementación pueden impactar en la efectividad de coste del sistema. El coste estimado deberá reevaluarse durante esta fase.

- Verificar los objetivos alcanzados en la implementación: El hecho de que se produzcan cambios continuos, influye en que el personal del proyecto ignore los objetivos del proyecto durante la fase de programación. El auditor debe controlar una implementación dirigida a cumplir los objetivos, ya que si los objetivos no se cumplen, el usuario tendrá la opción de solicitar cambios en el sistema.

- Implementar procedimientos que alcancen el cumplimiento de políticas, estándares y regulaciones. Si se detecta que no se están cumpliendo, se deberán tomar medidas adecuadas para alcanzar el grado de cumplimiento, llegando a modificar el sistema si fuese necesario.

IMPLEMENTAR CONTROLES DE INTEGRIDAD DE DATOS- 25		
Nº	*PREGUNTAS*	RESPUESTAS
1	¿Hay procedimientos escritos que indiquen cómo grabar las transacciones de entrada en sistemas automáticos? (Examinar si los procedimientos de entrada de datos son completos)	No
No existen procedimientos escritos a tales efectos.		
2	¿Han sido implementados los chequeos de validación de datos de entrada para asegurar que cumplen las especificaciones del sistema? (Revisar si los chequeos de validación de datos son completos)	Si
Si, en la práctica se implementan todos los controles necesarios para validar datos de entrada.		
3	¿Existen controles preventivos para asegurar que los datos válidos, pero no razonables, son anotados para una investigación manual? (Examinar la extensión de los controles preventivos para identificar los problemas potenciales)	Si
Si, dependiendo del tipo de aplicación. En programas que lo requieren por su importancia, se hacen chequeos.		
4	Los errores, ¿son identificados y explicados adecuadamente para que la acción correctora pueda realizarse pronto? (Examinar la utilidad de las listas y mensajes de error de datos)	Si
Si.		
5	¿Han sido establecidos procedimientos para realizar acciones correctivas sobre los errores en los datos? (Examinar si los procedimientos para abordar acciones correctivas al identificar errores son razonables)	No
No existen procedimientos documentalmente. No obstante se sigue el procedimiento de avisar sobre el error, designar a una persona responsable de solucionarlo y estudiar por qué ha ocurrido para evitar futuros errores.		
6	¿Hay procedimientos establecidos para asegurar que los errores son corregidos en un tiempo adecuado? (Verificar que los procedimientos aseguran que se corrigen los errores en un tiempo adecuado)	No
No existen procedimientos establecidos, pero en la práctica se corrigen en un tiempo mínimo.		
7	¿Existen controles punto a punto que aseguren la totalidad y exactitud de las transacciones al ser remitidas a otro punto del sistema? (Examinar si estos procedimientos son razonables)	Sí
Si, cuando existe un error de transmisión en el sistema se detecta. En ese caso se procede a la retransmisión.		
8	¿Se han implementado procedimientos que verifiquen los controles de entrada de datos instalados, tales como secuencias numéricas, números generados internamente, etc., para verificar que las entradas de registros son completas y exactas? (Verificar si los procedimientos y controles establecidos para verificar los datos durante su procesamiento, son adecuados)	Si
Si, existen procedimientos implementados para comprobar que las entradas son completas y exactas.		

En consecuencia, se recomienda:

- Establecer por escrito, documentalmente, procedimientos que definan el trato aplicado a las transacciones (controles realizados a las entradas, cómo se graban las entradas, etc.).

- Registrar en un documento los chequeos manuales realizados a ficheros que lo requieran: en qué fecha, qué persona lo realizó, etc.

- Hacer un registro de los errores encontrados en las aplicaciones, donde se haga constar la fecha en que se detecta el error, su origen, en qué fecha se corrige el error, quién se ocupa de solucionarlo, etc.

- Establecer procedimientos para realizar acciones correctivas sobre errores en los datos: registrarlos, corregirlos, etc.

- Establecer procedimientos por escrito para tener la certeza de que los errores se están corrigiendo en un tiempo aceptable.

MÉTODOS DE AUTORIZACIÓN -26		
Nº	*PREGUNTAS*	RESPUESTAS
1	¿Se han dividido los métodos de autorización entre manuales y automáticos? (Evaluar si los métodos de autorización elegidos son razonables)	No
No existen métodos de autorización.		
2	¿Se han preparado procedimientos para especificar el proceso de autorización manual para cada transacción? (Revisar la adecuación de esos procedimientos)	No
No existen métodos de autorización.		
3	¿Se han implementado los métodos en programas para autorizar transacciones en los segmentos automáticos del sistema? (Examinar las especificaciones del programa, o programas actuales, para determinar si el método de autorización ha sido correctamente implementado)	No
No existen métodos de autorización.		
4	¿Se han establecido procedimientos manuales que indiquen las transgresiones de los procedimientos de autorización manual? (Examinar si los procedimientos de trasgresión, para autorizaciones manuales, son razonables)	No
No existen métodos de autorización.		
5	¿Se han establecido procedimientos para identificar y actuar sobre las transgresiones, en los procedimientos de autorización automática? (Examinar si los procedimientos ante transgresiones de autorización automáticas, son adecuados)	No
No existen métodos de autorización.		
6	¿Están de acuerdo los métodos de autorización implementados con las normas de autorización definidas en la fase de requerimientos? (Verificar esa concordancia)	No
No existen métodos de autorización.		
7	¿Se han implementado procedimientos para verificar la fuente de las transacciones cuando a partir de la fuente se determina si la transacción está autorizada? (Verificar que el sistema autentifica la fuente de las transacciones, cuando es la propia fuente la que determina la autorización)	No
A partir de las fuentes no se determina si la transacción está autorizada.		
8	¿Mantiene el sistema un registro de quien autoriza cada transacción? (Verificar que los procedimientos se han implementado de tal forma que identifican quien autoriza cada transacción)	No
No, no se mantiene el registro.		

En consecuencia, se recomienda:

- Se cree conveniente que no todo el personal tenga acceso a los recursos del sistema y a realizar las transacciones que considere conveniente. Por ello, se recomienda definir procedimientos y normas de autorización, de tal manera que quede claramente definido qué personas están autorizadas para realizar qué tipo de transacciones. El sistema debería ser capaz de comprobar automáticamente si se trata de una persona autorizada, o no autorizada, y en consecuencia permitir o no permitir realizar la transacción.

- Establecer procedimientos para averiguar las transgresiones a los procedimientos de autorización.

CONTROLES DE INTEGRIDAD DE FICHEROS IMPLEMENTADOS -27		
Nº	*PREGUNTAS*	RESPUESTAS
1	¿Se ha señalado a alguien como responsable de la integridad de cada archivo? (Verificar que la persona asignada tiene el perfil adecuado y dispone del tiempo necesario)	Si
Si, normalmente las personas que trabajan con un archivo son responsables de la integridad de los mismos.		
2	¿Se han implementado controles de integridad de ficheros de acuerdo con los requerimientos de integridad de ficheros? (Comparar los controles implementados con los requerimientos de integridad establecidos en la fase de requisitos)	Si
Si, se implementan todos los controles de integridad de ficheros necesarios.		
3	¿Se han establecido procedimientos para notificar a la persona adecuada los problemas de integridad de archivos? (Examinar la adecuación de esos procedimientos)	No
No existen procedimientos por escrito. Normalmente se comunica directamente a la persona adecuada.		
4	¿Se han establecido procedimientos para verificar la integridad de los archivos de forma regular? (Revisar si la frecuencia de verificación de la integridad de los archivos es adecuada)	No
No, no existen procedimientos para verificarlo de forma regular. Se verifica en distintos puntos del ciclo de vida, según se considera necesario.		
5	¿Existen subsecciones o partes de archivos que deberían tener controles de integridad? (Confirmar con el usuario que todas las subsecciones o partes de los archivos tienen controles de integridad adecuados)	Si
Si, todas las partes de los archivos que lo requieren tienen sus propios controles de integridad.		
6	¿Existen procedimientos escritos para la conciliación regular entre los controles automáticos de archivos y todos los controles independientes? (Verificar si los procedimientos para reconciliar controles automáticos y controles manuales de mantenimiento, son razonables y puntuales)	No
No, no existen procedimientos escritos. No obstante cuando los controles automáticos detectan un error obligan a corregirlo instantáneamente.		
7	¿Se mantienen controles de integridad entre archivos, donde sean aplicables (por ejemplo, en las claves ajenas)? (Confirmar con el usuario que todas las relaciones entre ficheros están conciliadas en cuanto a integridad de ficheros se refiere)	Si
Si, se mantienen controles de integridad entre archivos de forma eficaz.		
8	Las transacciones importantes, ¿están sujetas a controles especiales de autorización? (Verificar con el asesor que los controles de autorización sobre transacciones importantes son adecuados)	No
No, las transacciones no están sujetas a controles especiales de autorización.		

En consecuencia, se recomienda:

- Sería conveniente que registrasen los controles realizados a los archivos, en qué momento se realizó, persona, etc.

- Establecer procedimientos para dar aviso de problemas de integridad de ficheros, de tal manera que estos queden registrados documentalmente, así como su resolución.

- Sería conveniente chequear la integridad de los ficheros de forma regular. Cuanto menos, asegurarse de que se vuelve a comprobar la integridad del fichero tras un cambio o al corregir un error.

RECORRIDO DE AUDITORÍA IMPLEMENTADO - 28		
Nº	*PREGUNTAS*	RESPUESTAS
1	Del trabajo trazado para la auditoría, ¿se han documentado las relaciones existentes en los controles, desde los controles en la fuente de registros hasta el control total? (Examinar si el recorrido de la auditoría es completo, desde la fuente del documento hasta el control total)	No
No, no se realizan auditorías, ni internas ni externas, siendo esta la primera auditoría realizada a la entidad. Por tanto no existe un trabajo trazado para la auditoría.		
2	¿Ha sido documentado el trabajo de auditoría, desde el control total hasta la fuente de las transacciones? (Examinar si el recorrido de la auditoría es completo, desde el control total hasta la fuente del documento)	No
No, no se realizan auditorías, ni internas ni externas, siendo esta la primera auditoría realizada a la entidad. Por tanto no existe un trabajo trazado para la auditoría.		
3	¿Han sido incluidos en el programa de auditoría todos los campos que se decidió incluir en el trabajo trazado para la auditoría? (Verificar que los registros del trabajo de auditoría incluyen todos los campos que fueron definidos para el trazado de trabajo de auditoría)	No
No, no se realizan auditorías, ni internas ni externas, siendo esta la primera auditoría realizada a la entidad. Por tanto no existe un trabajo trazado para la auditoría.		
4	El trabajo de auditoría implementado, ¿satisface la reconstrucción de requerimientos definida? (Verificar la concordancia entre el trabajo de auditoría implementado y la fase de reconstrucción de requerimientos)	No
No, no se realizan auditorías, ni internas ni externas, siendo esta la primera auditoría realizada a la entidad. Por tanto no existe un trabajo trazado para la auditoría.		
5	¿Han sido definidos procedimientos para hacer comprobaciones en el trabajo de auditoría? (Verificar que ha sido ideado un plan de listas de comprobación para el trabajo de auditoría)	No
No, no se realizan auditorías, ni internas ni externas, siendo esta la primera auditoría realizada a la entidad. Por tanto no existe un trabajo trazado para la auditoría.		
6	El trabajo de auditoría implementado, ¿permite la reconstrucción del proceso de transacción? (Revisar si los procesos de reconstrucción de transacciones son completos)	No
No, no se realizan auditorías, ni internas ni externas, siendo esta la primera auditoría realizada a la entidad. Por tanto no existe un trabajo trazado para la auditoría.		
7	El trabajo de auditoría realizado, ¿contiene la información necesaria para restablecer el entorno operacional después de un fallo? (Confirmar con el jefe de operaciones que la información es completa)	No
No, no se realizan auditorías, ni internas ni externas, siendo esta la primera auditoría realizada a la entidad. Por tanto no existe un trabajo trazado para la auditoría.		

En consecuencia, se recomienda:

- Crear una función interna de auditoría interna y realizar auditorías externas periódicas (por ejemplo, anualmente).
- Trazar un trabajo de auditoría al comienzo del ejercicio.
- Adquirir el material necesario para el proceso de auditoría.

PLAN DE CONTINGENCIA ESCRITO -29		
Nº	*PREGUNTAS*	RESPUESTAS
1	¿Identifica el plan de contingencia a las personas involucradas en el proceso de recuperación tras un fallo? (Confirmar con el jefe de operaciones que todas las personas adecuadas están identificadas en el plan de contingencia)	No
No, no se ha definido ningún plan de contingencia.		
2	¿Ha sido aprobado el plan de contingencia por el jefe de operaciones? (Examinar si hay evidencias que indiquen que el jefe de operaciones ha aprobado el plan)	No
No, no se ha definido ningún plan de contingencia.		
3	¿Identifica el plan todos los recursos necesarios para la recuperación? (Confirmar con el jefe de operaciones que todos los recursos necesarios están identificados)	No
No, no se ha definido ningún plan de contingencia.		
4	¿Incluye el plan de contingencia las prioridades para el restablecimiento de operaciones tras un fallo? (Revisar si las prioridades son razonables con el director)	No
No, no se ha definido ningún plan de contingencia.		
5	¿Especifica el plan de contingencia un lugar de procesamiento alternativo? (Confirmar si el lugar alternativo es adecuado para un proceso de back-up)	No
No, no se ha definido ningún plan de contingencia.		
6	¿Proporciona garantías el plan de seguridad durante el periodo de recuperación? (Revisar si el plan de seguridad es razonable con el jefe de seguridad)	No
No, no se ha definido ningún plan de contingencia.		
7	¿Ha sido desarrollado un plan para probar el plan de contingencia? (Examinar si el plan de comprobación es completo)	No
No, no se ha definido ningún plan de contingencia.		
8	¿Han sido incluidos en el plan de prueba los roles de partes externas a la entidad, tales como los proveedores de hardware, software, comunicaciones, y confirmado (el plan) por dichas partes? (Confirmar con las partes externas a la entidad que pueden aportar la ayuda indicada en el plan de contingencia)	No
No, no se ha definido ningún plan de contingencia.		

En consecuencia, se recomienda:

- Elaborar un plan de contingencia apropiado a la entidad.
- En el plan de contingencia que se elabore, identificar los recursos necesarios para la recuperación.

- Identificar las personas involucradas en el proceso de recuperación.
- Establecer las prioridades para el restablecimiento de operaciones tras un fallo.
- Especificar un centro de procesamiento alternativo. Se debe tener absoluta certeza de que este centro va a estar disponible caso de necesitarse.
- Tener en cuenta en el plan de contingencia todas las partes que se relacionan con la entidad.

PROCEDIMIENTOS DE NIVEL DE SERVICIO IMPLEMENTADOS -30		
Nº	*PREGUNTAS*	RESPUESTAS
1	¿Actúan los programas instalados de acuerdo con el nivel de servicio deseado? (Verificar los criterios de actuación de los programas durante las pruebas que se les realiza)	Si
Si, siempre se consigue el nivel de servicio acordado.		
2	La ejecución del sistema, ¿consigue el nivel de servicio deseado? (Verificar la ejecución del sistema durante las pruebas)	Si
Si, la ejecución del sistema consigue el nivel de servicio deseado.		
3	¿Han sido preparados programas de entrenamiento para las personas que usarán la aplicación del sistema? (Examinar si los programas de entrenamiento son completos)	Si
Si, existen programas de entrenamiento y se llevan a cabo.		
4	¿Está disponible el software de ayuda y cumple los requisitos de nivel de servicio? (Confirmar con el personal del área de operaciones que el software de ayuda está disponible y que cumple los criterios de actuación)	Si
Si, está disponible el software de ayuda y cumple los requisitos acordados.		
5	¿Está disponible el hardware de soporte y provee suficiente capacidad? (Confirmarlo con el personal del área de operaciones)	??
No suele haber hardware de soporte.		
6	¿Hay elementos hardware y software suficientes para anticiparse a futuros volúmenes? (Confirmarlo con operadores)	Si
Las aplicaciones software que se desarrollan son aptas para altos volúmenes de datos.		
7	¿Ha sido establecido un plan de comprobación para verificar que se pueden alcanzar los criterios de nivel de servicio? (Examinar si el plan de comprobación es completo)	No
No existe un plan de comprobación de forma documental, pero al aceptar un proyecto se sabe de antemano si se van a alcanzar los criterios de nivel de servicio demandados. Esto es así dada la experiencia del equipo en anteriores proyectos y al estudio previo que se realiza.		
8	Las entradas requeridas, ¿pueden ser procesadas a tiempo de tal forma que cumplan los planes de producción? (Confirmar con las personas que preparan las entradas si pueden hacerlo de tal forma que cumplan los planes de producción)	Si
Si, las entradas siempre son procesadas a tiempo.		

En consecuencia, se recomienda:

- Registrar en un documento los niveles de servicio demandados, así como establecer previamente un plan de comprobación que ayude a verificar que se alcanzan estos niveles de servicio.

PROCEDIMIENTOS DE SEGURIDAD IMPLEMENTADOS - 31		
Nº	*PREGUNTAS*	RESPUESTAS
1	¿Está el hardware de seguridad requerido disponible? (Confirmarlo con el jefe de seguridad)	Si
Si, tienen el hardware necesario de seguridad.		
2	¿Está el software de seguridad requerido disponible? (Confirmarlo con el jefe de seguridad)	No
No, considero que necesitarían software que registrase cambios realizados a los programas, que comparase códigos, que registrase transacciones, etc.		
3	¿Hay un procedimiento establecido para diseñar y mantener claves de acceso (contraseñas)? (Examinar si el procedimiento es completo y adecuado)	No
No, no existen procedimientos establecidos para el diseño y mantenimiento de claves de acceso.		
4	¿Ha sido entrenado el personal implicado en los procesos de seguridad? (Examinar si los procedimientos de entrenamiento sobre la seguridad son completos y adecuados)	No
No, el personal no ha sido entrenado en procedimientos de seguridad.		
5	¿Se ha establecido un procedimiento para gestionar y controlar las transgresiones de seguridad? (Examinar si el procedimiento de comprobación de transgresiones es completo y adecuado)	No
No, no se ha establecido un procedimiento para gestionar y controlar las transgresiones de seguridad.		
6	¿Ha sido mentalizada la dirección en los procedimientos para sancionar a los transgresores de la seguridad? (Confirmarlo con la dirección)	??
Dependiendo de la trasgresión, tomarían medidas oportunas.		
7	¿Han sido establecidos procedimientos para proteger los programas, listas de programas, documentaciones de datos y otros sistemas de documentación definiendo como trabaja el sistema? (Verificar con el jefe de seguridad la adecuación de los procedimientos de protección de los sistemas de documentación y programas)	No
No, no existen procedimientos establecidos para protegerlos.		
8	¿Ha sido señalado alguien como responsable de la seguridad de la aplicación cuando ésta llegue a ser operacional? (Verificar que el responsable tiene el perfil adecuado y dispone del tiempo necesario)	No
No, no existe una persona responsable de la seguridad.		

En consecuencia, se recomienda:

- Utilizar el software existente en la empresa: establecer claves de acceso en todos los equipos, controlar el acceso a las BD, etc.

- Adquirir software de seguridad complementario, que se considere útil para la entidad. Por ejemplo, que sea capaz de comparar dos versiones de programas, que sea capaz de detectar líneas fraudulentas (como ALTER OR MODIFY), que sea capaz de detectar e impedir grabar registros masivos de información, etc.

- Establecer un procedimiento para diseñar y mantener claves de acceso.

- Formar al personal en materia de seguridad de la información.

- Designar a alguna persona que tenga el perfil adecuado, como responsable de seguridad.

- Establecer un procedimiento para gestionar y controlar las transgresiones de seguridad.

- Establecer procedimientos para proteger los sistemas de información.

REEVALUACIÓN DE LA EFECTIVIDAD DE COSTES -32		
Nº	*PREGUNTAS*	RESPUESTAS
1	¿Se aproximan los costes de la fase de diseño y pruebas del sistema a los costes estimados? (Examinar el presupuesto del proyecto y verificar que los costes actuales se aproximan a los estimados)	Si
Si, tienen el hardware necesario de seguridad.		
2	¿Se aproximan los costes operacionales a los costes operacionales estimados? (Usar los datos del sistema de control de trabajo para comprobar que los costes actuales de prueba de operaciones se aproximan a los costes operacionales proyectados)	No
No, considero que necesitarían software que registrase cambios realizados a los programas, que comparase códigos, que registrase transacciones, etc.		
3	¿Son controlados los costes durante el desarrollo del proceso? (Confirmarlo con el jefe de proceso de datos)	No
No, no existen procedimientos establecidos para el diseño y mantenimiento de claves de acceso.		
4	¿Afectarán los cambios hechos durante la fase de programación a los costes estimados del sistema? (Confirmar con el jefe de proyecto que los cambios realizados durante la fase de programación, no afectarán a los costes operacionales)	No
No, el personal no ha sido entrenado en procedimientos de seguridad.		
5	¿Son aún razonables los beneficios estimados? (Confirmarlo con la dirección)	No
No, no se ha establecido un procedimiento para gestionar y controlar las transgresiones de seguridad.		
6	¿Es todavía razonable la vida prevista del proyecto? (Confirmarlo con la dirección de usuario)	??
Dependiendo de la trasgresión, tomarían medidas oportunas.		
7	¿Está planificado el proyecto teniendo en cuenta los días laborables, la fecha de inicialización y de fin, los recursos disponibles y las precedencias entre tareas? (Comparar el estado actual con el previsto en la planificación)	No
No, no existen procedimientos establecidos para protegerlos.		
8	¿Hay algún cambio esperado en las fases de prueba o de implantación, que pudiera afectar a los beneficios estimados sobre la inversión? (Confirmar con el jefe del proyecto si esto podría pasar)	No
No, no existe una persona responsable de la seguridad.		

2.3. CUESTIONARIOS VACÍOS

VERIFICAR LOS OBJETIVOS A LOGRAR EN LA IMPLEMENTACIÓN -33		
Nº	*PREGUNTAS*	RESPUESTAS
1	¿Se han dado cambios en la dirección del usuario que hayan afectado a los objetivos del sistema? (Confirmar con la dirección del usuario que los objetivos establecidos son los deseados)	
2	El programa implementado, ¿cumple con los objetivos establecidos? (Comparar los resultados del programa con los objetivos marcados)	
3	¿Son auditables los sistemas implementados? (Verificarlo)	
4	¿Se han producido los informes deseados? (Confirmar que los informes realizados por la aplicación del programa cumplen las especificaciones definidas por el usuario)	
5	Las entradas al sistema, ¿consiguen la consistencia de datos deseada y ofrecen fiabilidad en los resultados? (Confirmarlo con el usuario)	
6	El manual de usuario, así como todos los documentos que se producen como salida hacia el usuario, ¿son adecuados? (Confirmarlo con el usuario)	
7	¿Son los manuales y procedimientos de entrada adecuados para asegurar la preparación de datos válidos? (Confirmarlo con los preparadores de entradas)	
8	El usuario que estuvo involucrado en el proceso de desarrollo, ¿ha continuado estándolo en la fase de programación? (Confirmar con el personal de proyecto que la participación del usuario ha sido adecuada para asegurar su satisfacción)	

PROCEDIMIENTOS DE CONFORMIDAD - 34		
Nº	*PREGUNTAS*	RESPUESTAS
1	¿Han sido incorporadas en los programas de aplicación las políticas y procedimientos de la organización? (Examinar los programas para asegurar que están provistos de las políticas y procedimientos necesarios)	
2	¿Han sido incorporados en los programas de aplicación las políticas y procedimientos de procesamiento de datos de la empresa? (Examinar los programas para asegurarlo)	
3	¿Han sido incorporados en los programas de aplicación las políticas y procedimientos de control de la empresa? (Examinar los programas para asegurarlo)	
4	¿Han sido incorporadas a los programas de aplicación las regulaciones gubernamentales aplicables? (Examinar los programas para asegurarlo)	
5	¿Han sido incorporados a los programas de aplicación los estándares de la industria aplicables? (Examinar los programas para asegurarlo)	
6	¿Han sido incorporados a los programas de aplicación las políticas y procedimientos de la empresa del usuario? (Examinar los programas para asegurarlo)	
7	¿Son las políticas, procedimientos y regulaciones usadas como base para las especificaciones del sistema en la versión más actual? (Confirmarlo con las partes apropiadas)	
8	En el transcurso de tiempo que discurre entre la fase actual y el día en que el sistema se encuentre operativo, ¿se prevén cambios en las políticas, estándares o regulaciones? (Confirmar con las partes involucradas la posibilidad existente de cambios, o los cambios conocidos, en políticas, estándares o regulaciones que puedan ocurrir antes de que el sistema sea operacional)	

- FASE DE ACEPTACIÓN

Las pruebas de aceptación dan la oportunidad al usuario de verificar si el sistema cumple los requerimientos previstos. Este hito, que se desempeña al final de la fase de programación, se realiza para evitar la posibilidad de ofrecer al usuario como producto final, un sistema no apropiado para sus fines. Al concluir esta fase el cliente habrá aceptado, rechazado, o habrá señalado ciertas condiciones adicionales, necesarias para que el sistema sea adecuado para la producción.

Durante esta fase, el personal de procesamiento de datos, probará el sistema de acuerdo a las especificaciones iniciales, tal y como las entendieron. Si las pruebas realizadas durante el desarrollo se llevaron a cabo perfectamente, durante esta fase el sistema podría estar libre de errores. Sin embargo hay que tener en cuenta que las tareas a realizar y los cumplimientos de plazos de tiempo planificados no siempre permiten que las pruebas se realicen de una forma adecuada.

El departamento del usuario suele realizar pruebas al sistema para determinar si éste cumple los requisitos de acuerdo a sus necesidades. Debido a problemas de comunicación, es posible que existan diferencias entre las especificaciones iniciales con las que se construyó el sistema y los requerimientos que el usuario espera ver satisfechos. En este sentido podrían darse problemas.

Las pruebas de aceptación podrían llevarse a cabo ante el usuario y el personal de operaciones. El usuario preparará datos (que podrían ser reales), los introducirá en el sistema y verificará los resultados.

Esta fase consume un tiempo y un coste. Algunas organizaciones realizan en la fase de análisis las pruebas de aceptación y posteriormente continúan desarrollando pruebas de aceptación bajo distintas circunstancias, en la fase de diseño y programación.

El auditor revisará: El plan de pruebas de aceptación, las fechas de las pruebas de aceptación, los resultados obtenidos y por último el informe del usuario aceptando o rechazando la aplicación.

En esta fase el auditor podrá encontrarse ante dos situaciones: la primera ser el responsable y estar obligado a firmar el informe donde conste si el sistema es adecuado para la producción del cliente; y la segunda ofrecer una opinión sobre si el control es adecuado. Naturalmente en el primer caso su grado de participación en esta fase será más fuerte.

El auditor debe verificar que se ha preparado un plan adecuado de pruebas de aceptación y que se está usando. También verificará que existe una participación activa por parte del cliente o usuario. Revisará las pruebas realizadas y podrá recomendar áreas para hacer pruebas con mayor grado de profundidad, si lo considera adecuado.

PRUEBAS DE RECHAZO - 35		
Nº	*PREGUNTAS*	RESPUESTAS
1	¿Han sido probados datos que no están conformes a las especificaciones individuales de datos de cada elemento? (Verificar que los programas de validación de datos rechazan los datos que no son conformes a las especificaciones de los datos)	
2	¿Se han hecho pruebas que verifiquen las relaciones entre los datos, para comprobar que se rechazan aquellos datos que no cumplen las especificaciones del sistema? (Verificar que el sistema rechaza aquellas relaciones entre datos que no están de acuerdo con las especificaciones del sistema)	
3	¿Se han probado identificadores que no sean válidos? (Verificar que el programa rechaza estos identificadores)	
4	¿Se han realizado pruebas que verifiquen que las pérdidas en las secuencias de datos son detectadas? (Confirmar que el sistema detecta pérdidas en la secuencia de números)	
5	¿Se han realizado pruebas que aseguren, que los totales inexactos producidos en procesos internos, serán detectados? (Verificar que el sistema los detecta)	
6	¿Se han realizado pruebas que determinen que los datos perdidos en un proceso interno o de procesamiento, serán detectados? (Verificar que el programa detectará los datos perdidos en procesos internos)	
7	¿Se han realizado pruebas que detecten que las partes fijas del sistema no serán afectadas por datos no válidos? (Realizar pruebas de regresión que aseguren que las partes fijas del programa no se verán afectadas por datos inválidos)	
8	¿Se han realizado pruebas que verifican que los datos para, y desde otros programas, serán procesados adecuada y completamente? (Verificar que la interconexión entre sistemas funciona correctamente)	

COMPROBAR LA CONFORMIDAD – 36		
Nº	*PREGUNTAS*	RESPUESTAS
1	¿Aseguran los procedimientos manuales que se recibe la autorización adecuada? (Comprobar los procedimientos manuales para verificar que siguen los procedimientos de autorización)	
2	¿Se han probado las normas relativas a autorizaciones automáticas? (Verificar que los programas hacen cumplir las normas de autorizaciones automáticas)	
3	¿Han sido incluidos como parte de la prueba los nombres e identificadores actuales? (Confirmar que los identificadores actuales han sido incluidos en los programas)	
4	¿Se han introducido en el sistema operaciones no autorizadas para ver si son rechazadas? (Verificar que el programa las rechaza)	
5	Si se requieren varias autorizaciones, ¿funcionan los procedimientos adecuadamente? (Verificar que los procedimientos de autorización múltiple funcionan adecuadamente)	
6	Si quienes autorizan están limitados en el tamaño de operación que pueden autorizar, ¿se han introducido múltiples operaciones por debajo de este límite, para determinar si el sistema las detecta? (Verificar que el sistema identifica transgresiones potenciales de los límites de autorización, causadas por entradas de múltiples operaciones por debajo del límite)	
7	¿Han sido probados procedimientos para cambiar el nombre o el identificador de las personas autorizadas, para cambiar una transacción? (Verificar que las procedimientos de un programa, para cambiar las normas de autorización, funcionan adecuadamente)	
8	¿Han sido probados los procedimientos para informar a la dirección de las transgresiones de autorización? (Comprobar que los informes de trasgresión de autorizaciones son preparados adecuadamente y enviados)	

COMPROBAR LA INTEGRIDAD DE CONTROL -37		
Nº	*PREGUNTAS*	RESPUESTAS
1	¿Se han probado los controles de equilibrio entre archivos? (Verificar que los procesos de equilibrio de archivos funcionan correctamente)	
2	¿Se han probado todos los controles que se mantienen independientemente? (Verificar que estos controles pueden confirmar los controles totales sobre archivos)	
3	¿Se preparan informes cuando la integridad de los archivos se pierde? (Crear una condición que destruya la integridad de los archivos automáticos para determinar que se producen mensajes adecuados ante la pérdida de integridad)	
4	¿Se han probado procedimientos de integridad para asegurar que las actualizaciones son correctamente grabadas? (Verificar que todos los nuevos controles reflejan adecuadamente las operaciones de actualización)	
5	¿Se han realizado pruebas para asegurar que se retiene la integridad después de un fallo de programa? (Provocar un fallo en el programa para determinar si afecta a la integridad de los archivos)	
6	¿Se han introducido datos erróneos para determinar si pueden destruir la integridad de los archivos? (Introducir datos erróneos para determinar que no puedan afectar a la integridad de ficheros)	
7	¿Se han probado los procedimientos manuales que ofrezcan controles independientes? (Verificar que los procedimientos manuales pueden ser realizados adecuadamente para producir controles totales independientes correctos)	
8	Si múltiples archivos contienen el mismo dato, ¿serán cambiados todos los datos concurrentemente para asegurar la integridad de todos los archivos? (Cambiar un elemento de datos en un archivo, tal que sea redundante y se encuentre en distintos archivos, para verificar que en los demás archivos el cambio se producirá de la misma forma)	

COMPROBAR EL TRABAJO DE AUDITORÍA -38		
Nº	*PREGUNTAS*	RESPUESTAS
1	¿Se ha realizado una prueba para verificar que a los documentos fuente se les realizarán controles totales? (Verificar que una fuente de transacción determinada pasará los controles apropiados)	
2	¿Se ha realizado alguna lista de comprobación para verificar que todos los datos de ayuda para un control total, pueden ser identificados? (Determinar que para un control total todas las operaciones de ayuda pueden ser identificadas)	
3	¿Puede ser reconstruido el proceso de una única transacción? (Verificarlo)	
4	¿Se ha realizado alguna lista de comprobación para verificar que el trabajo de auditoría contiene la información apropiada? (Examinar el programa de auditoría para verificar que contiene la información apropiada)	
5	El trabajo de auditoría, ¿será guardado por un período de tiempo adecuado? (Verificarlo)	
6	¿Se han probado los procedimientos de trabajo de auditoría para determinar que las personas puedan reconstruir un proceso, desde los procedimientos del trabajo de auditoría? (Verificar que usando los procedimientos del trabajo de auditoría, las personas pueden reconstruir un proceso)	
7	¿Se ha construido alguna lista de comprobación para comprobar si el uso del trabajo de auditoría es rentable? (Determinar los costes de uso de los programas de auditoría para determinar que su uso es económico)	
8	¿Satisface el trabajo de auditoría los requisitos de auditoría? (Verificar con los auditores que el trabajo de auditoría satisface sus propósitos)	

ALTERNAR PRUEBAS DE PROCESAMIENTO Y DE RECUPERACIÓN -39		
Nº	*PREGUNTAS*	RESPUESTAS
1	¿Se ha creado un desastre simulado para probar los procedimientos de recuperación? (Crearlo y comprobar que se puede recuperar todo después de un desastre)	
2	¿Saben las personas cómo realizar una operación de recuperación desde los procedimientos de recuperación? (Verificar que la recuperación puede hacerse directamente a partir de los procedimientos de recuperación)	
3	¿Se ha diseñado alguna prueba para determinar si la recuperación se puede realizar dentro del periodo deseado de tiempo? (Realizar una prueba de recuperación para determinar que se puede realizar dentro de ese periodo de tiempo)	
4	¿Se ha entrenado al personal de operaciones en los procedimientos de recuperación? (Confirmar que el personal ha recibido ese entrenamiento)	
5	¿Se ha probado cada tipo de fallo de sistema? (Verificar que el sistema puede recuperarse de cada uno de los tipos de fallos de sistema)	
6	¿Se han probado los procedimientos manuales de back-up para los fallos de sistema? (Simular un desastre de sistema para comprobar que los procedimientos manuales son adecuados)	
7	¿Se han probado los procedimientos manuales para la entrada de datos recibidos en el sistema (mientras el sistema está caído) después de que la integridad del sistema halla sido restablecida? (Verificar que los usuarios del sistema pueden introducir adecuadamente los datos que han sido acumulados durante un fallo del sistema)	
8	¿Pueden ser realizados procedimientos de procesamiento alternativos usando procedimientos manuales? (Exigir procedimientos de procesamiento manual alternativos)	

HACER HINCAPIÉ EN LAS PRUEBAS -40		
Nº	*PREGUNTAS*	RESPUESTAS
1	¿Se han documentado los límites de todas las tablas internas y otras restricciones de volumen? (Verificar con el jefe del proyecto que todos los límites están documentados)	
2	¿Se han realizado listas de comprobación para probar cada uno de los límites documentados? (Verificar que los límites de aplicación han sido probados)	
3	¿Se han incluido procedimientos programados para comprobar que las transacciones que no pueden ser procesadas con la capacidad actual, son retenidas para un procesamiento posterior? (Confirmar que cuando se introducen más transacciones de las que el sistema puede manejar, éstas son almacenadas para un procesamiento posterior)	
4	La parte de entradas del sistema, ¿ha sido sometida a pruebas especiales? (Verificar que entradas excesivas no causarán problemas en el sistema)	
5	¿Ha sido sometida a pruebas especiales la parte manual del sistema? (Verificar que cuando las personas realizan más transacciones de las que se pueden procesar, éstas no se pierden)	
6	¿Se han realizado pruebas especiales para probar las comunicaciones del sistema? (Verificar que cuando se requiere que los sistemas de comunicaciones realicen más transacciones de las que permite su capacidad, éstas no se pierden)	
7	¿Se han escrito procedimientos trazando los procesos a ser seguidos cuando el volumen excede la capacidad del sistema? (Evaluar si los procedimientos de exceso de capacidad son razonables)	
8	¿Se han desarrollado pruebas usando personal auxiliar, para verificar que el sistema puede procesar volúmenes normales sin que esté presente el personal regular? (Probar el funcionamiento del sistema cuando es operado por personal auxiliar que pueda ser requerido en situaciones de emergencia)	

PRUEBAS SOBRE LAS TRANSGRESIONES AL SISTEMA -41		
Nº	*PREGUNTAS*	RESPUESTAS
1	¿Se han identificado los riesgos de seguridad? (Examinar la totalidad de estos riesgos)	
2	¿Se han hecho pruebas que transgredan la seguridad física? (Intentar transgredir la seguridad física para determinar si la seguridad es adecuada)	
3	¿Se han realizado pruebas para transgredir la seguridad de acceso? (Realizar procedimientos que transgredan la seguridad de acceso de forma controlada, para probar si estos procedimientos son adecuados)	
4	¿Se han realizado pruebas para comprobar si los recursos del ordenador pueden ser usados sin autorización? (Intentar utilizar los recursos de un ordenador sin la adecuada autorización)	
5	¿Han sido realizadas pruebas para determinar si los procedimientos de seguridad son adecuados durante las horas no laborables? (Realizar transgresiones a la seguridad durante las horas no laborables para determinar si los procedimientos de seguridad funcionan bien)	
6	¿Se han realizado pruebas repetitivas para intentar transgredir la seguridad mediante continuos intentos? (Realizar este tipo de intentos para determinar si así se puede romper la seguridad)	
7	¿Han sido realizadas pruebas para obtener el acceso a los programas y sistemas de documentación? (Intentar conseguir ese acceso)	
8	¿Están correctamente entrenados los empleados en los procedimientos de seguridad? (Verificar que los empleados conocen y siguen los procedimientos de seguridad)	

VERIFICAR LOS COSTES Y LOS BENEFICIOS -42		
Nº	*PREGUNTAS*	RESPUESTAS
1	¿Pueden operar los sistemas con una ayuda anticipada manual? (Verificar que los sistemas se pueden utilizar con un esfuerzo manual anticipado)	
2	¿Se pueden procesar las transacciones dentro de los costes estimados? (Verificar que los costes del procesamiento de transacciones están dentro de las tolerancias estimadas)	
3	¿Se ha realizado la fase de pruebas dentro del presupuesto establecido para ello? (Verificar con los informes de control que la fase de pruebas se ha realizado dentro de su presupuesto)	
4	¿Se han encontrado problemas en las pruebas que afecten a la eficiencia en costes del sistema? (Confirmar con el jefe del proyecto que los problemas detectados no afectarán significativamente a la eficiencia en costes del sistema)	
5	¿Indica la fase de pruebas que los beneficios estimados serán los reales? (Confirmarlo con la dirección del usuario)	
6	Los cambios proyectados en el hardware y el software, ¿reducirán significativamente los costes de mantenimiento y operacionales? (Confirmarlo con operaciones en el ordenador)	
7	¿Existen pruebas en la planificación basada en identificar tareas, personas, presupuestos y costes? (Examinar la totalidad de la fase de pruebas sobre la planificación)	
8	La tecnología utilizada para la implementación, ¿es multimedia? (Confirmar con una fuente independiente si se han considerado aspectos que puedan ser importantes, como la sonoridad del sistema)	

PRUEBAS FUNCIONALES -43		
Nº	*PREGUNTAS*	RESPUESTAS
1	Los procedimientos que originan transacciones normales, ¿están de acuerdo con las especificaciones? (Verificar que los procedimientos que originan transacciones están de acuerdo con los requerimientos del sistema)	
2	¿Funcionan los procedimientos de entrada de acuerdo a las especificaciones? (Verificar que los procedimientos de entrada funcionan de acuerdo a los requerimientos del sistema)	
3	¿Funcionan los procedimientos de procesamiento de acuerdo a las especificaciones? (Verificar que los procedimientos de procesamiento funcionan de acuerdo a los requerimientos del sistema)	
4	¿Funcionan los procedimientos de retención en almacenes de acuerdo a las especificaciones? (Verificar que los procedimientos de retención en almacenes funcionan en concordancia con los requerimientos del sistema)	
5	¿Funcionan los procedimientos de salida de acuerdo a las especificaciones? (Verificar que los procedimientos de salida funcionan en concordancia con los requerimientos del sistema)	
6	¿Funcionan los procedimientos de error manual de acuerdo a las especificaciones? (Verificar que los procedimientos de error manual son detectados en concordancia con los requerimientos del sistema)	
7	¿Funcionan los procedimientos de comunicación de acuerdo a las especificaciones? (Verificar que los procedimientos de comunicación funcionan de acuerdo con los requerimientos del sistema)	
8	¿Funcionan los procedimientos de retención de datos de acuerdo a las especificaciones? (Verificar que los procedimientos de retención de datos funcionan de acuerdo a los requerimientos del sistema)	

COMPROBAR LA CONFORMIDAD -44		
Nº	*PREGUNTAS*	RESPUESTAS
1	¿Verifican las pruebas que el sistema de procesamiento está de acuerdo con las políticas y procedimientos de la empresa? (Verificar que los resultados del sistema operacional están de acuerdo con las políticas y procedimientos de la empresa)	
2	¿Verifican las pruebas que el sistema de procesamiento está de acuerdo con las políticas y procedimientos de procesamiento de datos? (Verificar que los resultados del sistema operacional están de acuerdo con las políticas y procedimientos de procesamiento de datos)	
3	¿Verifican las pruebas que el sistema de procesamiento está de acuerdo con las políticas y procedimientos de control? (Verificar que los resultados del sistema operacional están de acuerdo con las políticas y procedimientos de control)	
4	¿Verifican las pruebas que el sistema de procesamiento está de acuerdo con las regulaciones gubernamentales? (Verificar que los resultados del sistema operacional están de acuerdo con las regulaciones gubernamentales)	
5	¿Verifican las pruebas que el sistema de procesamiento está de acuerdo con los estándares de la industria? (Verificar que los resultados del sistema operacional están de acuerdo con los estándares de la industria)	
6	¿Verifican las pruebas que el sistema de procesamiento está de acuerdo con las políticas y procedimientos del usuario? (Verificar que los resultados del sistema operacional están de acuerdo con las políticas y procedimientos del usuario)	
7	¿Están de acuerdo los procedimientos de pruebas con el plan de pruebas? (Verificar que el plan de pruebas está totalmente instalado)	
8	¿Han verificado las pruebas que la integridad de los datos está adecuadamente protegida? (Confirmar con el usuario si las pruebas son completas, para verificarlo)	

- REVISAR LA FASE DE CONVERSIÓN

Se establecerán los requerimientos de la fase de conversión y se diseñará el mecanismo para instalar el nuevo sistema. Es posible que se deba programar para convertir los ficheros existentes y en tal caso estos programas deberán probarse antes de ejecutar la conversión.

El auditor revisará si la conversión se realiza completamente y si los cambios sobre datos y ficheros, realizados durante esta fase, son adecuados y completos.

En la fase de conversión debe conseguirse un sistema operacional:

- Si es necesario, para ello se cambiarán fechas antiguas a un nuevo formato, lo cual puede suponer realizar un programa que lea de los registros antiguos y que cree nuevos registros.
- Puede que el nuevo sistema necesite datos adicionales, en cuyo caso se necesitarán nuevos programas para validar los nuevos datos.
- Los nuevos programas deberán situarse en producción, cuando los antiguos programas sean borrados de producción.
- Se deberán instalar nuevas instrucciones para los usuarios de la aplicación.

El proceso de conversión puede ser difícil de ejecutar dentro de las restricciones de tiempo. Por ejemplo, hay conversiones que se llevan a cabo durante el fin de semana. Pero si la conversión no ha sido completada con éxito durante esos dos días la organización puede encontrarse con serios problemas el lunes por la mañana. Algunas organizaciones adoptan un método ante esta circunstancia: se escoge de antemano un período de tiempo en el que el nuevo sistema deberá haberse instalado con éxito. De no ser así, realizan la vuelta a atrás y continúan utilizando el viejo sistema.

El auditor esperará encontrar los siguientes entregables:

- El plan de conversión.
- El diagrama de flujo de la fase de conversión.
- Listas de programas de conversión con su correspondiente documentación.
- Documentos que reflejen los movimientos de los programas dentro de producción y el borrado de programas.
- Nuevas instrucciones para el operador.
- Nuevas instrucciones y procedimientos de usuario.
- Procedimientos para verificar que la conversión se ha llevado a cabo con éxito.

El auditor deberá asegurar que existe un plan adecuado, con procedimientos adecuados y que es posible realizar el esfuerzo necesario, todo ello para minimizar el número de problemas que puedan ocurrir después de que el sistema sea operacional.

El auditor podrá ser incluido en la planificación para la conversión, para asegurar la integridad de los ficheros y que el proceso se está llevando a cabo adecuadamente, dada su independencia.

Verificará que se cumplan los siguientes objetivos:

Que la integridad de los datos de los archivos esté asegurada durante el proceso de conversión, que los programas estén instalados en la fecha marcada en la planificación, que se haya formado al personal y que existan posibilidades de volver al sistema antiguo.

VERIFICAR LA EXACTITUD Y COMPLETITUD DE LA CONVERSIÓN -45		
Nº	*PREGUNTAS*	RESPUESTAS
1	¿Han sido identificados los archivos que necesitan ser convertidos? (Confirmar con el jefe del proyecto que se han identificado todos los archivos)	
2	¿Han sido identificados los registros que necesitan cambios? (Confirmar con el jefe del proyecto que se han identificado todos los registros y los datos que necesitan cambios)	
3	¿Han sido desarrollados e implementados procedimientos para verificar que los cambios realizados a los datos sean exactos y completos? (Examinar si las rutinas de validación de datos están completas)	
4	¿Han sido adecuadamente probadas las rutinas de conversión y validación de los datos? (Examinar si el plan de pruebas y los resultados obtenidos son completos)	
5	¿Ha sido señalado un individuo como responsable para verificar que los datos han sido convertidos exacta y completamente? (Determinar si esta persona tiene el perfil adecuado y el tiempo necesario para desempeñar esta función)	
6	¿Se han establecido controles para asegurar que todos los datos necesarios para ser introducidos en el archivo a convertir, han sido incluidos en el archivo? (Examinar la adecuación de los procedimientos y seleccionar un ejemplo del archivo convertido para determinar que contiene todos los datos necesarios)	
7	¿Están correctamente identificados todos los errores encontrados durante la conversión? (Revisar los procedimientos de error y los listados de errores para estar seguros de que están completos y son útiles)	
8	¿Son todos los errores corregidos e introducidos de nuevo, antes de terminar el proceso de conversión? (Verificar con un ejemplo básico que los errores detectados han sido corregidos e introducidos antes de terminar la fase de conversión)	

CAMBIOS DE DATOS PROHIBIDOS DURANTE LA CONVERSIÓN -46		
Nº	*PREGUNTAS*	RESPUESTAS
1	¿Verifican los procedimientos que la entrada de nuevos datos durante la conversión está autorizada? (Verificar la adecuación de los procedimientos de autorización en la conversión)	
2	¿Puede una persona ser identificada como quien autorizó los nuevos datos durante el proceso de conversión? (Confirmar con un ejemplo básico que los nuevos datos pueden ser rastreados hasta la persona que autorizó la inclusión de esos datos)	
3	¿Está prohibida la inclusión de nuevas entidades de control tales como empleados, clientes, etc., durante el proceso de conversión? (Verificar con ejemplos que no hay nuevas entidades que hayan sido introducidas durante el proceso de conversión)	
4	¿Está prohibida la alteración, inserción o borrado de los datos financieros durante el proceso de conversión? (Verificarlo con ejemplos)	
5	¿Han sido autorizados por la dirección del usuario, los cambios hechos a los datos (por ejemplo, un nuevo campo de datos)? (Confirmarlo con la dirección del usuario)	
6	¿Han sido autorizados los cambios en la longitud y estructura de los campos? (Confirmarlo con la dirección del usuario)	
7	¿Han sido autorizadas las inclusiones de nuevos códigos, divisiones de control, etc.? (Confirmar con las partes indicadas que los nuevos códigos, control de entradas, etc. han sido autorizadas.)	
8	Si ocurren borrados, añadidos o modificaciones a entidades de control, tales como registros de clientes, o datos financieros, etc. ¿están adecuadamente autorizados? (Confirmar si ha habido cambios y en caso afirmativo, si están apropiadamente autorizados.)	

VERIFICAR LA INTEGRIDAD EN LA PRODUCCIÓN DE FICHEROS -47		
Nº	*PREGUNTAS*	RESPUESTAS
1	¿Han sido documentados todos los controles de integridad sobre archivos? (Confirmar si los controles sobre la integridad de ficheros son correctos)	
2	¿Han sido identificados los archivos que pueden ser modificados, antes de usarlos con los nuevos sistemas? (Confirmar con la dirección de usuario que la lista de archivos es completa)	
3	¿Puede ser usada una simple prueba de control (por ejemplo, antiguo archivo de saldo, más las inserciones, menos los borrados, igual al nuevo archivo de saldo), para verificar la integridad de la nueva versión del archivo? (Examinar si la prueba de control es adecuada)	
4	¿Se pueden ajustar los totales de archivos independientes, en base a los cambios ocurridos durante la conversión? (Confirmar con el responsable de los totales que ese total será mantenido durante la conversión)	
5	¿Se ha señalado a una persona como responsable de verificar la integridad de los archivos al terminar el proceso de conversión? (Confirmar que esta persona tiene el perfil adecuado y el tiempo necesario)	
6	¿Han sido establecidos procedimientos para identificar las pérdidas de integridad de ficheros? (Revisar si las rutinas de identificación de pérdidas de integridad son adecuadas)	
7	¿Se han establecido procedimientos para mantener la integridad de los archivos manuales durante la conversión? (Verificar la adecuación de los procedimientos y probar que la integridad de los archivos manuales ha sido verificada al concluir la fase de conversión)	
8	¿Ha sido probada la integridad de los archivos maestros al finalizar el proceso de conversión? (Verificar la adecuación de los procedimientos y comprobar la integridad de los archivos maestros)	

AUDITORÍA EN LA CONVERSIÓN -48		
Nº	*PREGUNTAS*	RESPUESTAS
1	¿Se mantienen las versiones antiguas de los archivos producidos después de la fase de conversión? (Confirmar con el personal de operaciones que se guardan por un tiempo razonable los antiguos archivos)	
2	¿Se guardan los antiguos programas? (Confirmar con el personal de operaciones que se guardan por un tiempo razonable)	
3	¿Existe un programa de auditoría que retenga los cambios hechos a los archivos? (Confirmar en el registro de operaciones del ordenador que se registran los cambios en los archivos)	
4	¿Existe un programa de auditoría que mantenga los cambios producidos a programas operacionales? (Confirmar en las operaciones del ordenador que se puede mantener un registro de los cambios del programa por un periodo razonable de tiempo)	
5	¿Existe un programa de auditoría que mantenga los cambios realizados a una parte manual de la aplicación? (Confirmar con la dirección de usuario que un programa de auditoría puede mantener los cambios al sistema manual)	
6	¿Hay alguien responsable de definir y asegurar que el programa de auditoría ha sido creado? (Verificar que existe esa persona y que tiene el perfil adecuado y el tiempo necesario)	
7	¿Existe un programa de auditoría que registre las funciones operacionales durante el proceso de conversión? (Confirmar en las operaciones del ordenador que se puede mantener un registro de las acciones)	
8	¿Se ha señalado a alguien que retenga la información del programa de auditoría durante los cambios de conversión, hasta que la integridad del nuevo sistema sea probada? (Verificar que existe una persona con la autoridad de retener la información del programa de auditoría hasta que la integridad del nuevo sistema haya sido probada)	

ASEGURAR LA INTEGRIDAD DEL SISTEMA ANTERIOR -49		
Nº	*PREGUNTAS*	RESPUESTAS
1	¿Se han retenido los programas del sistema anterior en un estado que permita reactivarlos en el caso en que sea necesario? (Confirmar con el personal de operaciones que se guardan los programas del sistema anterior)	
2	Las instrucciones de operación del antiguo sistema, ¿han sido retenidas en un estado que permita que sean reactivadas si fuese necesario? (Confirmar con el personal de operaciones que se han guardado las instrucciones de operación)	
3	Los archivos maestros del antiguo sistema, ¿han sido retenidos en un estado que permita que sean reactivados si fuese necesario? (Confirmar con el personal de operaciones que los ficheros maestros han sido guardados)	
4	Los archivos de transacciones recogidas del sistema antiguo, ¿han sido retenidos en un estado que permita que sean reactivados si fuese necesario? (Confirmar con el personal de operaciones que los archivos de transacciones fueron retenidos)	
5	Los procedimientos de operación manual del antiguo sistema, ¿fueron retenidos en un estado que permita que sean reactivados si fuese necesario? (Confirmar con el personal de operaciones que los procedimientos de operación manual son retenidos)	
6	¿Se han mantenido controles externos e independientes sobre totales y procedimientos para reconciliar esos totales? (Confirmar con la persona responsable del control total independiente que no hay pérdida de integridad sobre los totales)	
7	¿Se le han notificado al usuario las especificaciones que no han sido implementadas? (Confirmar con el personal del proyecto que se le han notificado al cliente todas las especificaciones que no han sido implementadas)	
8	¿Se ha designado personal con experiencia en proyectos para mantener el sistema? (Confirmar con el personal del proyecto que los miembros con experiencia pueden ser asignados para la fase de mantenimiento)	

GRABACIONES ANTE FALLOS EN EL PLAN DE CONVERSIÓN -50		
Nº	*PREGUNTAS*	RESPUESTAS
1	¿Ha sido documentado cada paso de la conversión en la secuencia con la cual se ejecuta? (Examinar si el plan de conversión es adecuado)	
2	¿Se ha asignado un tiempo estimado a cada paso del plan de conversión? (Examinar el plan de conversión para corroborar que se ha asignado un tiempo estimado para cada paso)	
3	¿Se ha desarrollado un plan para volver al antiguo sistema en el caso en que la conversión no se realice con éxito? (Examinar el plan de vuelta al antiguo sistema en casos en que la conversión no se realiza con éxito)	
4	¿Se ha asignado un tiempo estimado para el plan de conversión del antiguo sistema? (Examinar el tiempo asignado en el plan)	
5	¿Se ha determinado un punto a partir del cual se pueda volver al antiguo sistema en casos en que la conversión no se haya desarrollado con éxito? (Examinar el plan para determinar que se ha identificado el punto a través del cual se realizará la vuelta al antiguo sistema)	
6	A partir del punto de retorno al antiguo sistema, ¿existe suficiente tiempo para realizar la vuelta atrás antes de la necesidad de comenzar con la producción? (Calcular según el plan de conversión que se ha previsto suficiente tiempo para volver al antiguo sistema sin incidir en el estado de la producción)	
7	¿Se ha señalado a una persona como responsable de la toma de decisiones de vuelta al antiguo sistema? (Determinar si la persona responsable tiene suficiente autoridad como para tomar la decisión de volver al antiguo sistema)	
8	¿Se ha establecido un procedimiento para notificar las partes involucradas que pueden estar en producción a partir del siguiente día? (Examinar en qué medida es completo el procedimiento para notificar las distintas partes con las que el sistema de producción puede ser reemplazado)	

SEGURIDAD EN LA CONVERSIÓN -51		
Nº	*PREGUNTAS*	RESPUESTAS
1	¿Se han definido y se han dado a conocer los requerimientos de seguridad de la aplicación del sistema en el período de conversión? (Confirmar con el usuario que la clasificación de seguridad definida es adecuada y que el período de conversión es suficiente)	
2	¿Se invocan procedimientos para proteger la seguridad de los datos en programas, durante el proceso de conversión? (Revisar si los procedimientos de seguridad son adecuados y observar la implementación de estos procedimientos de seguridad)	
3	¿Se ha señalado a una persona como responsable de la seguridad durante el proceso de conversión? (Confirmar que la persona responsable tiene suficiente autoridad y el tiempo suficiente para desarrollar esta función)	
4	Si la información almacenada en medios provisionales ya no es necesaria, ¿se han purgado los datos del medio provisional o de paso? (Verificar que existen procedimientos para purgar los datos importantes de los medios intermedios y que esos procedimientos se siguen)	
5	¿Se registran las acciones de operación durante el proceso de conversión? (Confirmar que se produce un registro durante el proceso de conversión)	
6	¿Se revisa el registro producido durante el proceso de conversión para asegurar que no han ocurrido acciones inválidas? (Confirmar que el registro ha sido revisado por un responsable con suficiente conocimiento)	
7	¿Se ha establecido un procedimiento para registrar los intentos de transgresiones a la seguridad durante el proceso de conversión) (Examinar si el procedimiento de seguridad ante transgresiones es razonable)	
8	¿Los documentos de control son almacenados en un área segura? (Examinar la seguridad del área donde se almacenan los documentos de control)	

DESARROLLO DEL PRESUPUESTO DE CONVERSIÓN -52		
Nº	*PREGUNTAS*	RESPUESTAS
1	¿Se ha establecido un presupuesto para el proceso de conversión? (Examinar la existencia de un presupuesto de conversión)	
2	El presupuesto de conversión, ¿es adecuado para desarrollar y llevar a cabo una fase de conversión controlada? (Confirmar con el jefe de proyecto y el jefe de operaciones que el presupuesto de conversión es adecuado)	
3	¿Prevé aspectos de seguridad el presupuesto de conversión? (Determinar si el presupuesto de conversión tiene en cuenta aspectos de seguridad)	
4	El presupuesto de conversión, ¿tiene en cuenta los programas de auditoría necesarios? (Determinar si el presupuesto de conversión tiene en cuenta los programas de auditoría)	
5	El presupuesto de conversión, ¿tiene en cuenta los controles necesarios para asegurar la integridad de ficheros? (Determinar si el presupuesto de conversión tiene en cuenta los controles de integridad sobre archivos)	
6	El presupuesto de conversión, ¿tiene en cuenta verificar si la conversión se ha realizado adecuadamente y de forma completa? (Determinar si el presupuesto de conversión tiene en cuenta las verificaciones para que la conversión se realice de forma exacta y completa)	
7	Los fondos para la conversión, ¿son usados en la fase de conversión? (Revisar los asientos contables para asegurar que los fondos asignados a la conversión no son usados en otras fases)	
8	¿Existe una planificación de la fase de conversión que identifique tareas, personas, presupuestos y costes? (Examinar si el programa de trabajo para la fase de conversión está completo)	

IDENTIFICAR PROBLEMAS EN LA CONVERSIÓN -53		
Nº	*PREGUNTAS*	RESPUESTAS
1	¿La dirección ha señalado a una persona responsable del proceso de conversión, con conocimientos suficientes sobre la aplicación y que disponga de tiempo suficiente para dirigir la conversión? (Verificar que la persona tiene los conocimientos necesarios sobre la aplicación y que tiene suficiente autoridad y tiempo para supervisar el proceso de conversión)	
2	¿Se han establecido criterios para determinar cuándo se ha realizado la conversión con éxito? (Examinar si el criterio de aceptación de la conversión es razonable)	
3	¿Se ha desarrollado un procedimiento para comunicar los problemas de conversión al área usuaria? (Examinar si la comunicación del informe de errores es razonable y funciona)	
4	¿Se han establecido procedimientos para asegurar que se van a realizar las acciones necesarias ante los errores antes de dar paso a la producción? (Confirmar con la dirección del usuario que se ha realizado el plan de acciones sobre los errores antes de emplazar el nuevo sistema en la producción)	
5	¿Se han identificado las nuevas funciones del sistema para que puedan ser gestionadas después de que el sistema entre en la producción? (Determinar que se han identificado los posibles problemas previstos)	
6	¿Se han asignado personas para revisar los posibles problemas previstos una vez que el sistema se introduzca en la producción? (Determinar que se han asignado personas para revisar los problemas potenciales, después de que el sistema entre en producción; y que estas personas han sido informadas de los problemas potenciales)	
7	¿Se ha establecido un proceso para comunicar los problemas que puedan surgir después de la instalación, al personal del proyecto? (Determinar si los canales de comunicación de problemas al personal del proyecto son adecuados)	
8	¿Se ha llevado a cabo una auditoría después de la instalación para determinar que el sistema funciona en la producción en concordancia con los requerimientos? (Verificar que se ha llevado a cabo una auditoría después de la instalación)-	

ASEGURAR EL ACATAMIENTO DE LOS PROCEDIMIENTOS DE CONVERSIÓN -54		
Nº	*PREGUNTAS*	RESPUESTAS
1	¿El departamento de procesamiento de datos, dispone de los procedimientos de conversión? (Examinar si los procedimientos de conversión de los datos son completos)	
2	¿Ha preparado el usuario procedimientos para la conversión de programas? (Examinar si los procedimientos de conversión del usuario son completos y probar la conformidad con estos procedimientos)	
3	Los procedimientos de conversión, ¿aseguran que las nuevas versiones de los programas pueden estar en producción en el tiempo apropiado? (Examinar los listados de librerías del programa para verificar que las nuevas versiones del programa están en el estado de producción)	
4	¿Los procedimientos de conversión prevén ordenar suficientes cantidades de nuevos impresos y medios del ordenador? (confirmar con el área de operaciones que suficientes medios e impresos han sido ordenados)	
5	¿Los procedimientos de conversión prevén el etiquetado de los nuevos archivos? (Examinar los nuevos archivos para determinar si están etiquetados apropiadamente)	
6	¿Se ha informado a las áreas de soporte para el procesamiento de datos de los nuevos procedimientos que se necesitan para el nuevo sistema? (Confirmar con los grupos de soporte para el procesamiento de datos si están suficientemente preparados para dar soporte a la nueva aplicación del sistema)	
7	Los procedimientos de conformidad con el procesamiento de datos, ¿tienen en cuenta la actualización de los procedimientos operacionales asociados con el nuevo sistema? (Examinar los procedimientos operacionales y determinar si son actualizados)	
8	¿Existe un grupo de aseguramiento de la calidad, o el jefe de procesamiento de los datos, verifican la conformidad con los procedimientos de conversión? (Confirmar que una persona responsable del procesamiento de los datos verifica la conformidad con los procedimientos de conversión)	

2.4. OTROS POSIBLES CUESTIONARIOS

- Cuestionarios de determinación del nivel de acceso a los activos de información de la empresa. Deberá incluir el carácter público o privado de los resultados, se tendrá en cuenta el compromiso del personal, etc.

- Cuestionarios de establecimientos de políticas, procedimientos y metodologías. Incluirá disposiciones empresariales, normativas, etc.

- Cuestionarios sobre el registro de resultados. Incluirá evaluación del funcionamiento del sistema, tiempo de reacción, etc.

- Cuestionarios de control preventivo. Incluirá puntos sobre la asignación de responsabilidades, políticas de actuación, plan de contingencia, etc.

- Cuestionarios sobre el entorno de trabajo. Incluirá cuestiones referentes a la luminosidad, confortabilidad, ergonomía, etc.

- Cuestionarios sobre seguridad. Incluirá preguntas sobre las redes internas y externas, los back-up, los routers, antivirus, centros alternativos de trabajo, planes de contingencia, etc.

3. AUDIT SYSTEMS

3.1. INTRODUCCIÓN. METODOLOGÍA APLICADA.

Audit Systems es una aplicación informática que ha sido elaborada con el fin de apoyar a auditores expertos a lo largo de los procesos de auditoría.

A diferencia de otras aplicaciones, Audit Systems tiene distintas funcionalidades que se ejecutarán a lo largo de todo el proceso de auditoría:

1. Contiene la parte correspondiente a la metodología a aplicar: fase de análisis.

2. Es capaz de recoger datos de distintos usuarios: fase de toma de datos.

3. Es capaz de realizar una evaluación interna y generar recomendaciones y puntos que deben ser solventados: fase de revisión de resultados.

4. Es capaz de generar informes automáticamente con recomendaciones: fase de información.

En la fase de toma de datos Audit Systems utiliza unos cuestionarios que han sido incluidos en la aplicación para plantear preguntas dirigidas, en función del perfil del empleado que esté respondiendo.

Estos cuestionarios han sido realizados con una metodología basada en los Objetivos de Control para la Información y Tecnologías Relacionadas de ISACA, así como la Guía de Seguridad de SEDISI y se han cubierto los cuestionarios MARION.

Para la realización de sus funciones Audit Systems cuenta con tres módulos principales:

1. Módulo administrador: permite gestionar usuarios.

2. Módulo de procesamiento: para el procesamiento de los datos de los cuestionarios.

3. Módulo de informes: para la realización de informes automatizados como resultado de la auditoría.

En los siguientes apartados se explicará detalladamente el funcionamiento de cada uno de ellos.

Para ejecutar Audit Systems tras su instalación, bastará con hacer doble clic en el icono de instalación que se muestra en el escritorio:

Figura 15. Acceso a Audit Systems

Una vez ejecutado, se mostrará una ventana de acceso de usuario. Esta ventana permitirá el acceso:

1. Al módulo administrador, si el usuario y claves se corresponden a las del administrador de la aplicación.

2. Al módulo de procesamiento, si se trata de cualquier otro usuario.

3.2. MÓDULO ADMINISTRADOR.

El módulo administrador de Audit Systems es aquel que permite gestionar las cuentas de usuario para acceder a la aplicación. Para acceder a este módulo es necesario arrancar la aplicación con la cuenta de administrador.

Sus funciones principales son:

- Alta de usuario, asignación de perfil y de clave de acceso.
- Búsqueda y visualización de usuarios.
- Edición de datos de usuario.
- Borrado de usuarios.

Este módulo recibirá como entrada una petición de acceso al sistema. Se requerirá el nombre de la persona que se desea dar de alta, así como su cargo.

Internamente el cargo de una persona se utiliza para la asignación de un perfil de usuario. Estos perfiles están relacionados con una serie de cuestionarios, de tal forma que posteriormente en la fase de procesamiento se realizarán preguntas dirigidas en función del perfil de la persona que esté accediendo a la aplicación.

Así por ejemplo a un perfil administrativo no se le plantearán preguntas como si ha estudiado la adecuación de una metodología de trabajo frente a otra, - que se plantearía a un perfil de dirección -, ni contestará a cuestionarios donde se pregunte si ha desarrollado y probado un plan de contingencia de restauración de las bases de datos, - pregunta que iría dirigida a perfiles de los departamentos de informática y sistemas principalmente-.

Sí contestaría a otros tipos de cuestionarios como por ejemplo los referentes a la accesibilidad de la documentación, la confidencialidad de los documentos, etc.

Como salida ofrecerá el alta de un usuario en la aplicación, así como su correspondiente contraseña, o bien modificación a los datos del mismo.

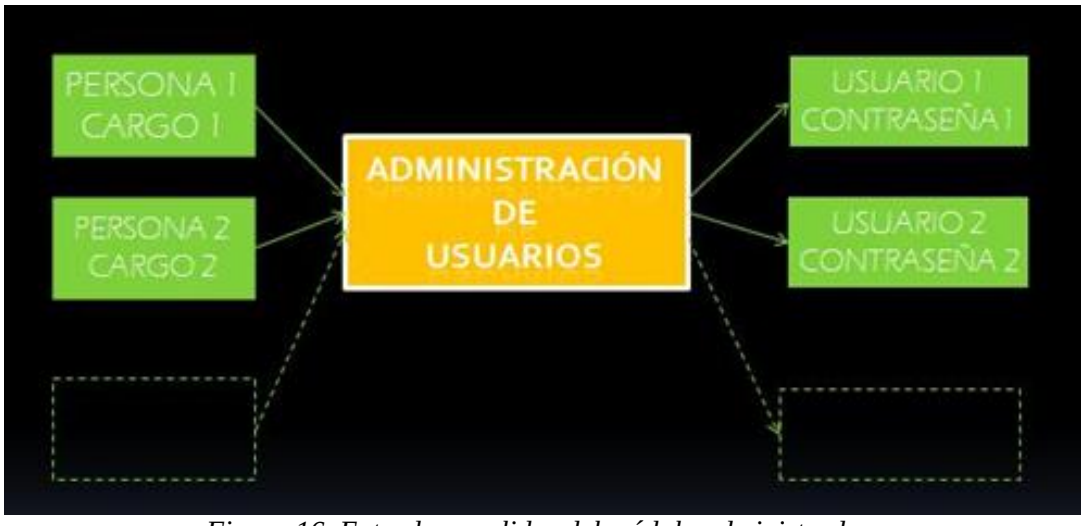


Figura 16. Entradas y salidas del módulo administrador.

Para acceder al módulo administrador de Audit Systems se hará doble clic sobre el ejecutable que se encuentra en el escritorio. Se mostrará entonces una ventana temporal que dará paso a la ventana de acceso de usuarios.

Figura 17. Ventana temporal de acceso.

Será necesario introducir un usuario asignado al perfil de administrador junto a la clave de acceso correcta.

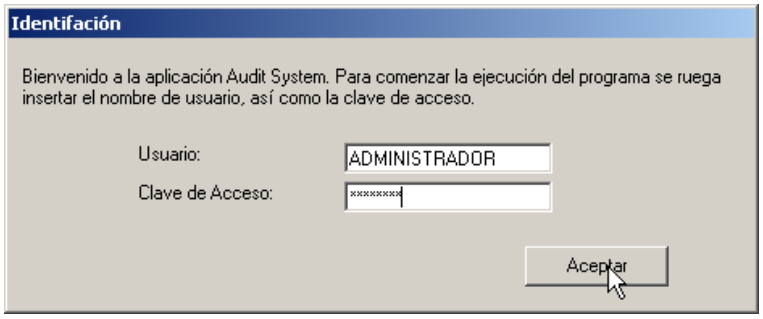


Figura 18. Ventana de acceso de usuarios.

Tanto si el usuario no es correcto, como si la contraseña es errónea, la aplicación mostrará un mensaje de advertencia y no permitirá el acceso.

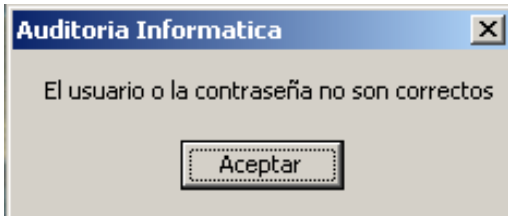


Figura 19. Ventana de error de acceso.

Si por el contrario tanto el usuario como la clave son correctos y además el usuario que se ha introducido tiene perfil de administrador, se accederá al módulo administrador de Audit Systems.

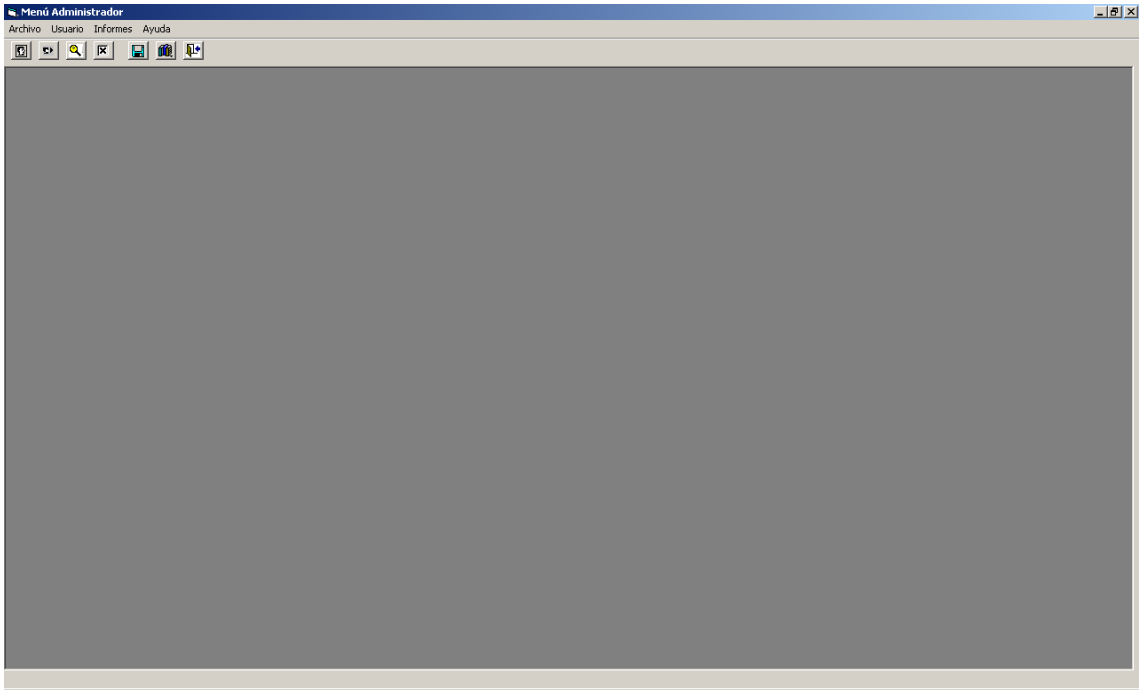


Figura 20. Módulo administrador.

Menú Principal.

El menú consta de cuatro accesos:

1. Archivo.
2. Usuario.
3. Informes.
4. Ayuda.

Menú Archivo.

El menú "Archivo", también accesible mediante el teclado "Alt + A", tiene dos entradas: guardar y salir.

Figura 21. Menú Archivo.

La entrada "**Guardar**", también accesible mediante el teclado "Ctrl + G", permite guardar los cambios que se hayan realizado hasta el momento.

El guardado también se podrá realizar a través del icono correspondiente de la barra de herramientas:

Figura 22.Guardar cambios.

La opción "**Salida**", también accesible mediante el teclado "Ctrl + S", permite salir de la aplicación finalizando la ejecución de Audit Systems. Se podrá salir también de la aplicación utilizando el icono correspondiente:

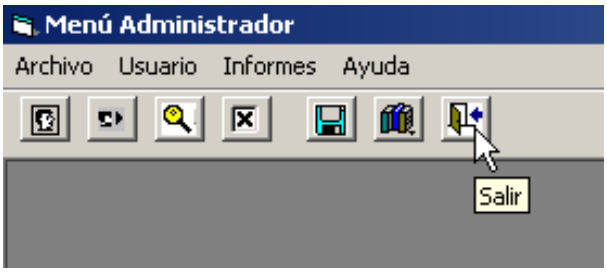


Figura 23. Salir de la aplicación.

Menú Usuario.

El menú "Usuario", también accesible mediante el teclado "Alt + U", dispone de cuatro entradas: alta de usuario, modificar usuario, visualizar usuario y baja de usuario.

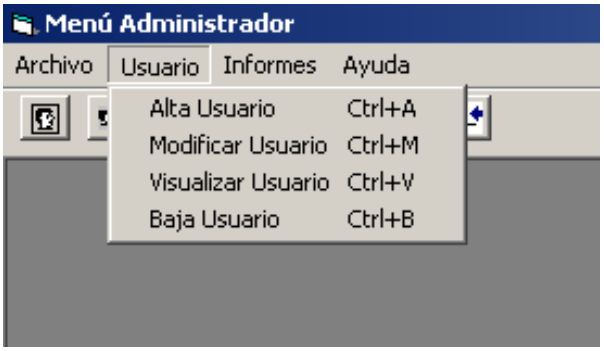


Figura 24. Menú usuario.

La entrada "**Alta Usuario**", también accesible mediante el teclado "Ctrl + A", permite dar de alta un nuevo usuario de la aplicación. Los empleados de una empresa auditada deberán ser dados de alta en el sistema con carácter previo al procesamiento de datos, a fin que puedan acceder a la aplicación.

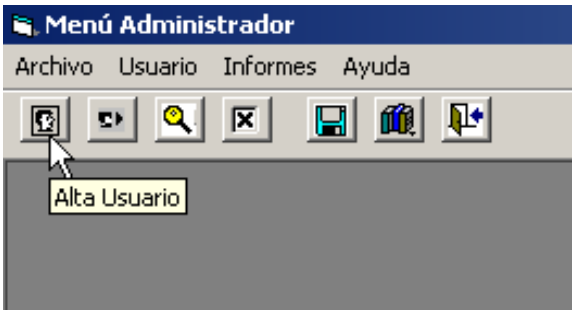


Figura 25. Alta de usuarios.

Como puede observarse en la imagen precedente también existe un icono en la barra de herramientas que permite acceder a la ventana de alta de usuario. Se mostrará entonces la siguiente ventana:

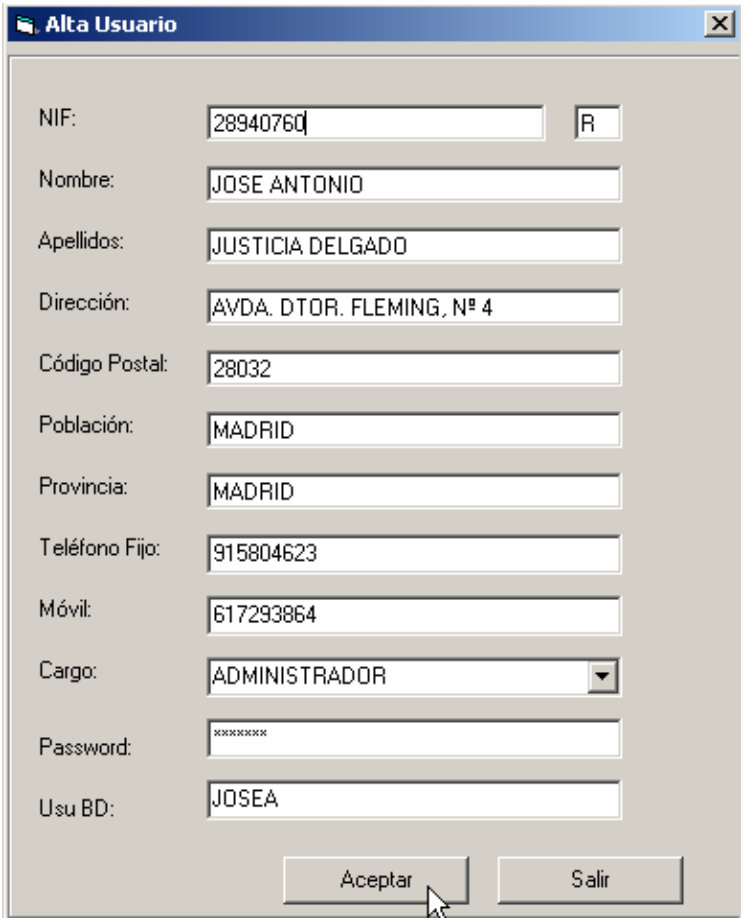


Figura 26. Ventana de alta de usuarios.

Se deberán rellenar los datos referentes al nuevo usuario. La tecla del tabulador permitirá al administrador desplazarse de celda en celda.

Como puede observarse en la imagen será necesario asociar un cargo al usuario que se está dando de alta. De este modo a través del cargo el usuario quedará asignado a un perfil de usuario, que a su vez está relacionado con una categoría de informes.

Estas relaciones permitirán en el módulo de procesamiento de datos la realización de preguntas dirigidas conforme al puesto de trabajo que desempeñe cada persona.

Por último se hará clic en el botón "Aceptar". Como medida de seguridad, para evitar errores en la introducción de la clave de acceso, se mostrará una ventana solicitando al administrador confirmar la contraseña de acceso.

Figura 27. Confirmar contraseña.

El administrador entonces volverá a incluir la contraseña en la ventana:

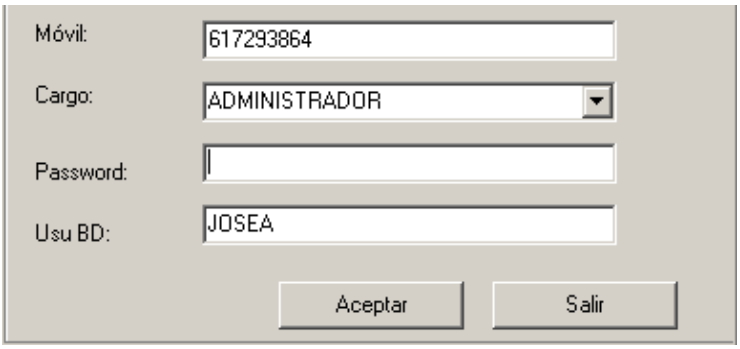


Figura 28. Repetir contraseña.

En el caso de error, se mostrará un mensaje de advertencia:

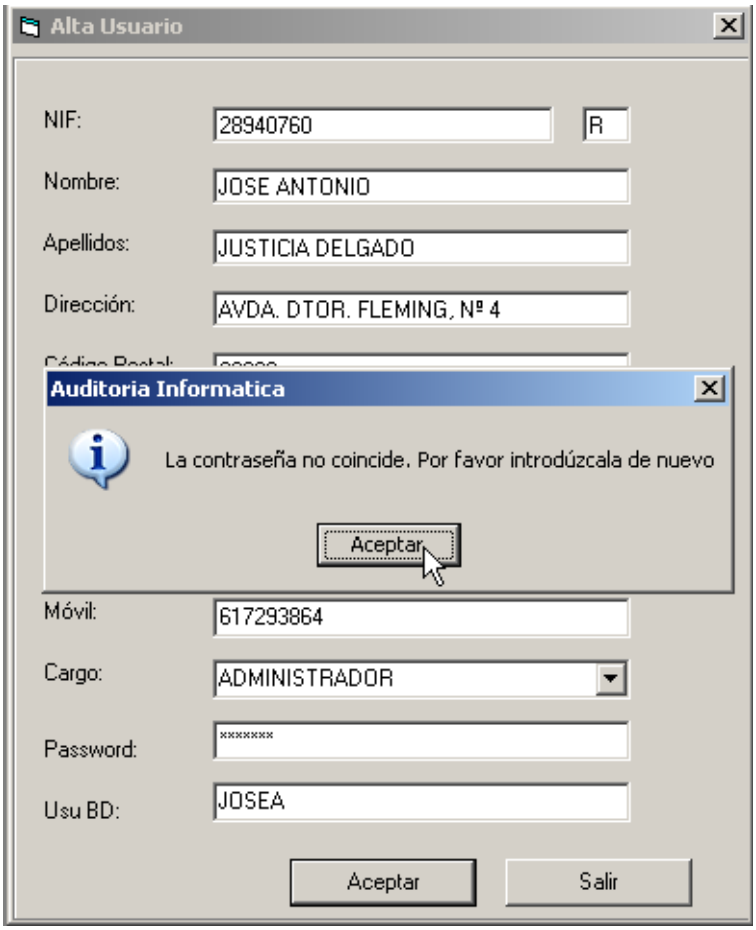


Figura 29. Error en la contraseña.

Si la contraseña es correcta, se mostrará un mensaje de confirmación de alta.

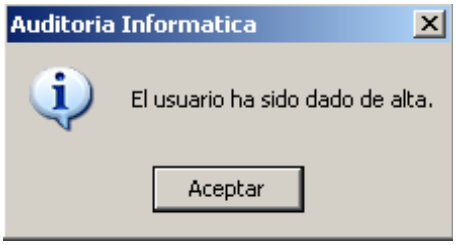


Figura 30. Confirmación alta usuario.

Una vez se muestre este mensaje, el nuevo usuario habrá sido dado de alta en el sistema. Entonces el administrador podrá proceder al comunicado de alta de usuario junto con la clave de acceso, advirtiendo que tanto el usuario como la clave deben ser personales e intransferibles.

La entrada del menú "**Modificar Usuario**", también accesible mediante el teclado "Ctrl + M", permite modificar los datos de un usuario existente en el sistema. Así por ejemplo si una persona cambiase de residencia, o de número de teléfono, se deberá acceder a esta ventana para actualizar los nuevos datos.

Figura 31. Modificar usuario.

Esta entrada del menú también tiene asociado un icono en la barra de herramientas:

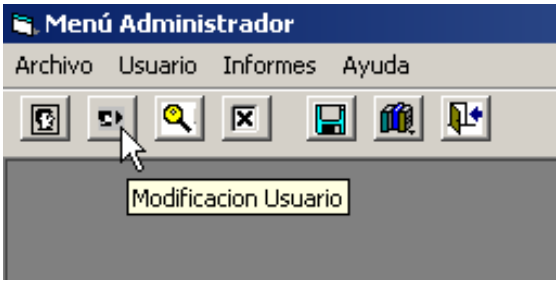


Figura 32. Acceso rápido modificar usuario.

Se mostrará entonces la siguiente ventana:

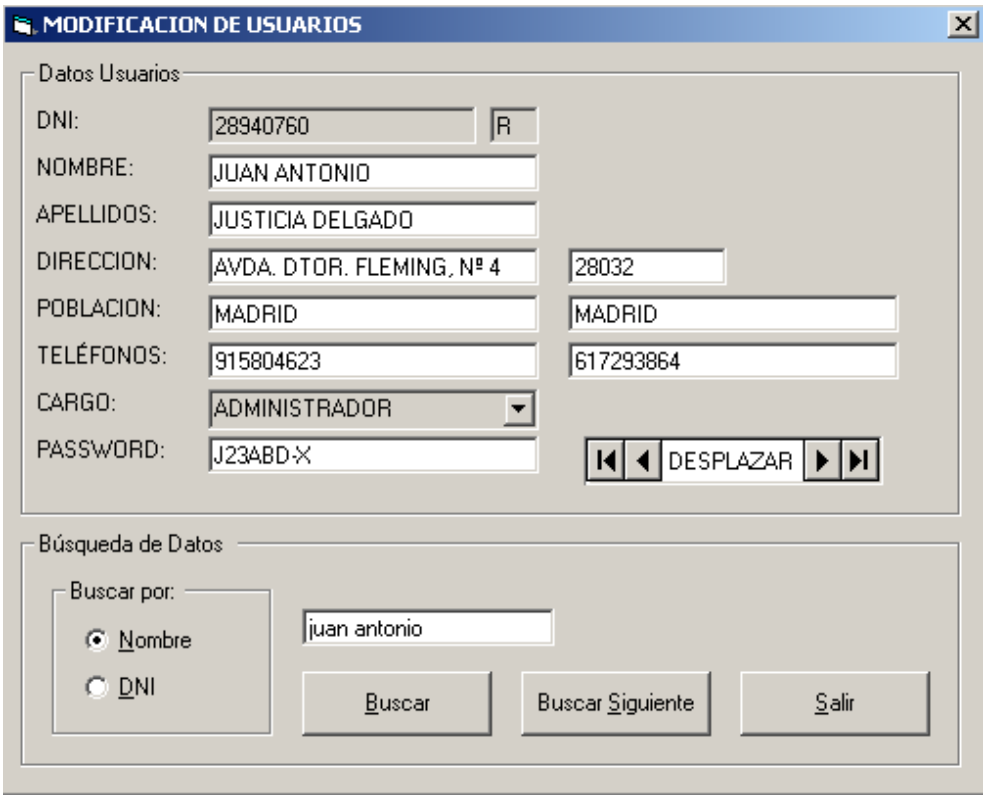


Figura 33. Ventana de modificación de usuarios.

Esta ventana ofrece al administrador las siguientes opciones:

1. Modificar la información del usuario, a excepción del DNI y del cargo asociado.
2. Desplazarse por cada uno de los registros y visualizar la información de cada uno de ellos.
3. Realizar una búsqueda en los registros existentes a través del Nombre o el DNI.
4. Salir de la ventana de modificación de usuarios.

Para **editar los datos** de un registro bastará con situarse con el ratón sobre la celda correspondiente y cambiar la información que se muestra.

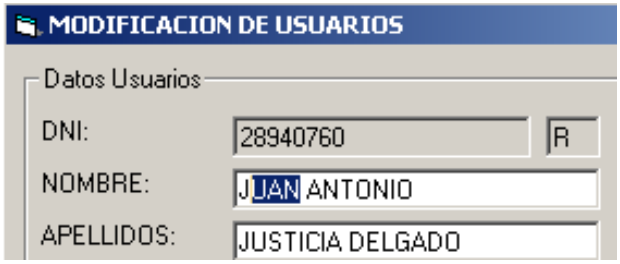


Figura 34. Edición de registro.

Téngase en cuenta que los campos sombreados, DNI y cargo, no podrán ser modificados. Si por alguna circunstancia fuese necesario modificar estos campos, se debería proceder dando de baja el usuario y dando de alta uno nuevo.

Para **desplazarse** entre los distintos registros el administrador utilizará la barra de desplazamiento.

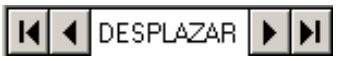


Figura 35. Barra desplazamiento.

De izquierda a derecha las flechas permiten:

1. Desplazarse al primer registro.
2. Ir al registro anterior.
3. Acceder al siguiente registro.
4. Posicionarse en el último registro.

Cada vez que se muestre un registro distinto, se visualizarán en la parte superior todos los datos del mismo.

No obstante esta barra de desplazamiento no permite la localización rápida de un registro. Para ello resulta más aconsejable utilizar la opción de búsqueda que ofrece la ventana en su parte inferior.

La **búsqueda de datos** permite dos opciones:

1. Búsqueda a través del nombre.
2. Búsqueda a través del DNI.

La búsqueda por nombre se encontrará activa por defecto. Para usarla bastará con introducir el nombre que se desea buscar y presionar sobre el botón “Buscar”.

Audit Systems localizará entonces el primer registro que ha sido introducido, cuyo nombre de usuario coincide con el nombre objeto de la búsqueda.

El usuario administrador comprobará entonces que se localiza el primer registro de la aplicación, si es que existe alguno; y además tendrá ocasión de comprobar que se muestra un nuevo botón que anteriormente no aparecía en la ventana: “Buscar siguiente”.

Este botón permite desplazarse al siguiente registro cuyo nombre coincide con el nombre que se está buscando.

Cada vez que la búsqueda encuentre un nuevo registro se irán visualizando todos los datos en la parte superior de la ventana. De esta forma el usuario administrador tendrá la probabilidad de editar los nuevos datos encontrados.

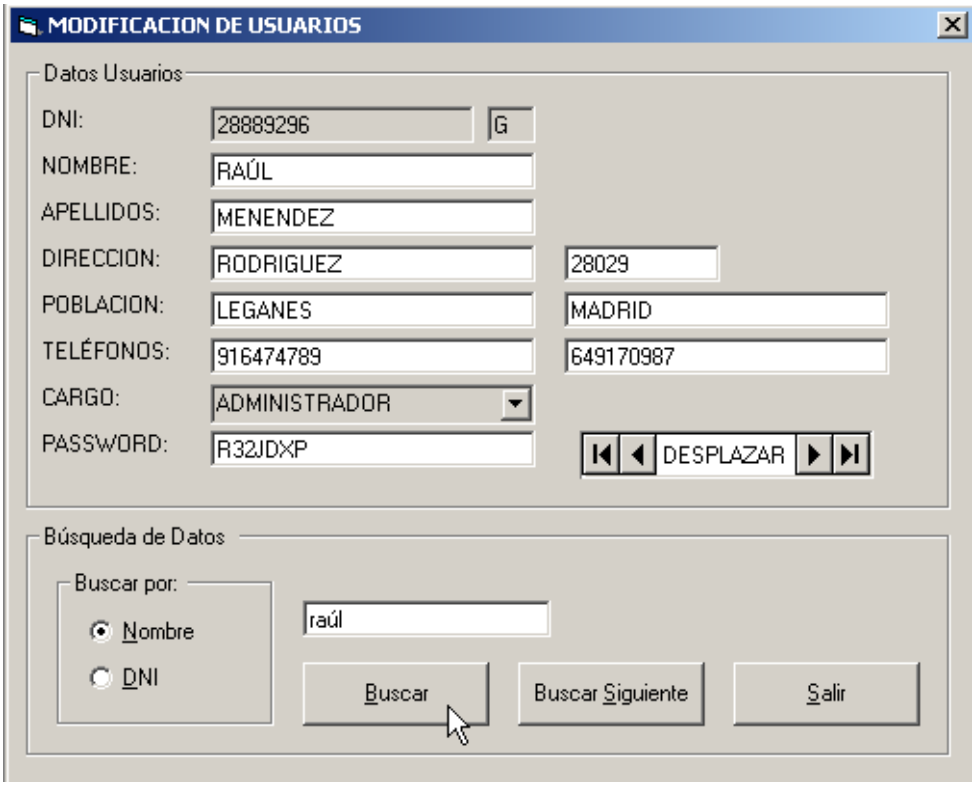


Figura 36. Búsqueda por nombre.

Para activar la opción de búsqueda por "DNI", bastará con seleccionar la opción con este mismo nombre. Se introducirá entonces el DNI sin letra final y se hará clic en el botón "Buscar".

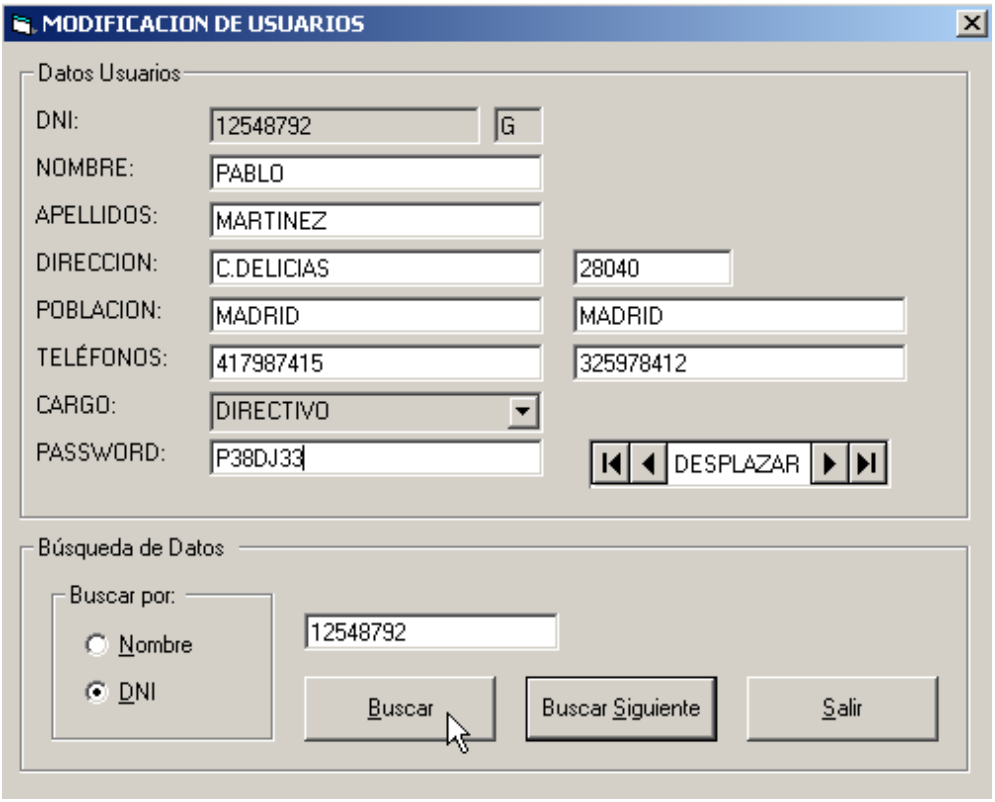


Figura 37. Búsqueda por DNI.

Se mostrará entonces el registro con el DNI que se está buscando, o bien un mensaje informativo advertirá que no hay registros con ese DNI.

Una vez finalizadas las ediciones, para salir de la ventana de modificación de datos el administrador usuario hará clic en el botón "Salir". Volverá a encontrarse en la pantalla principal de administración.

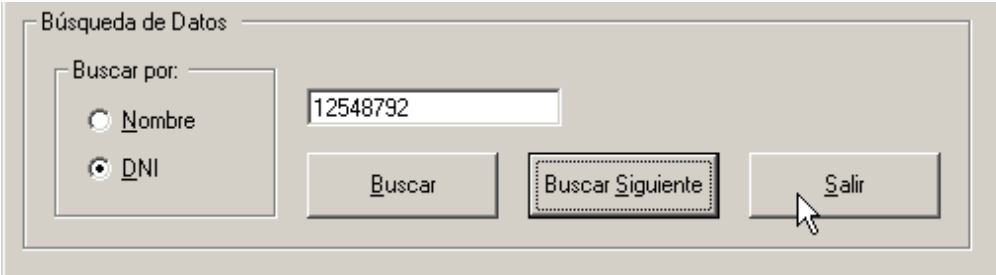


Figura 38. Salir ventana modificación usuarios.

La entrada del menú "**Visualizar Usuario**", también accesible mediante el teclado "Ctrl + V", permite visualizar los datos de un usuario existente en el sistema. Esta funcionalidad es recomendable para la consulta de información, dado que no permite la edición de datos y por tanto se evita que el usuario administrador, por error, pueda variar o borrar algún dato.

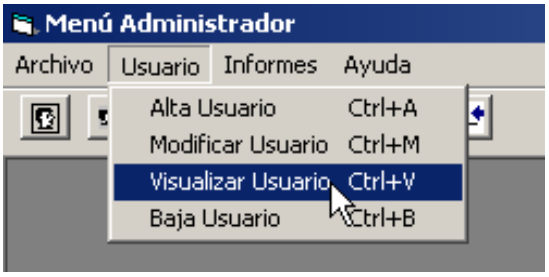


Figura 39. Visualizar usuario.

Esta entrada del menú también tiene asociado un icono en la barra de herramientas:

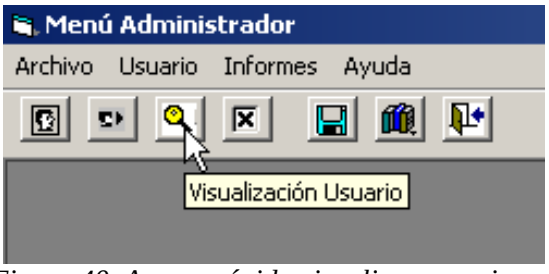


Figura 40. Acceso rápido visualizar usuario.

Al acceder a la funcionalidad, ya sea a través del menú o bien a través del icono de la barra de herramientas, se mostrará la siguiente ventana.

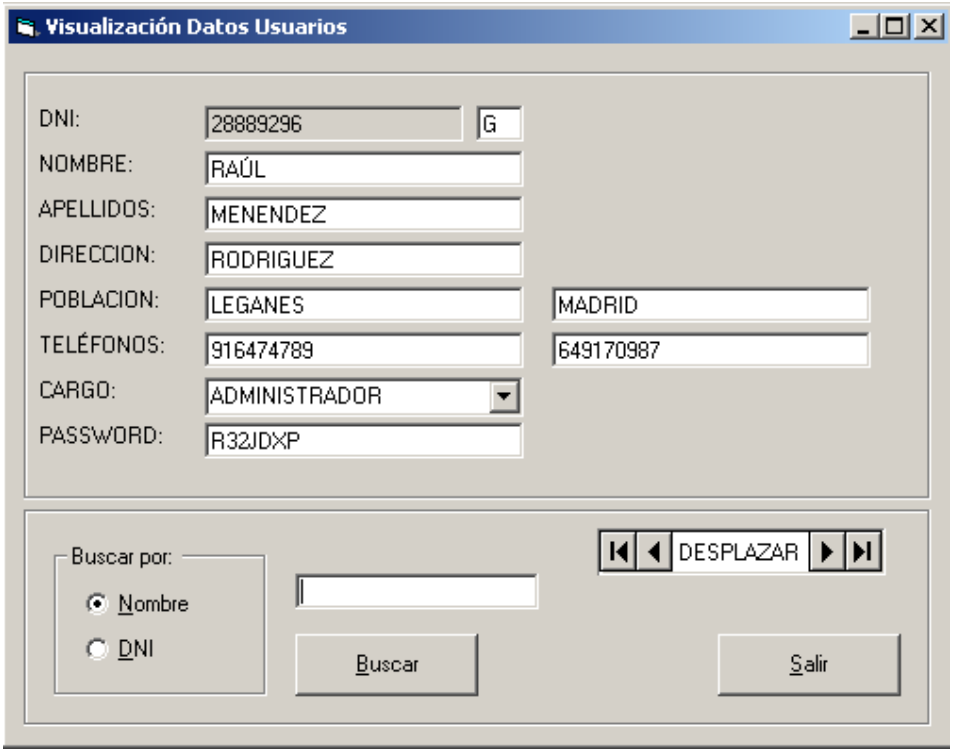


Figura 41. Ventana visualización usuario.

Como puede observarse la ventana es bastante similar a la ventana de modificación de usuarios, si bien como se dijo anteriormente esta ventana resulta más segura para la consulta de datos, puesto que no permite la edición de los mismos.

Las funcionalidades que ofrece son las siguientes:

1. Consulta de datos de los usuarios dados de alta.
2. Desplazamiento en los registros.
3. Búsqueda de registros a través del nombre.
4. Búsqueda de registros a través del DNI.
5. Salir de la ventana.

Para informarse sobre el funcionamiento de estas funcionalidades será necesario revisar la ventana anterior de modificación de usuarios.

La entrada del menú "**Baja Usuario**", también accesible mediante el teclado "Ctrl + B", permite dar de baja a un usuario existente. Esta funcionalidad es aplicable, por ejemplo, cuando una persona ha dejado de trabajar en la empresa auditada.

Figura 42. Baja usuario.

Esta entrada del menú también tiene asociado un icono en la barra de herramientas:

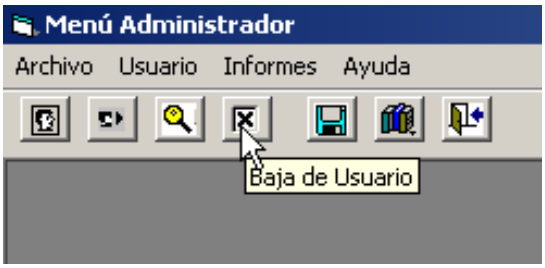


Figura 43. Acceso rápido baja usuario.

Al seleccionar la entrada se mostrará la siguiente ventana:

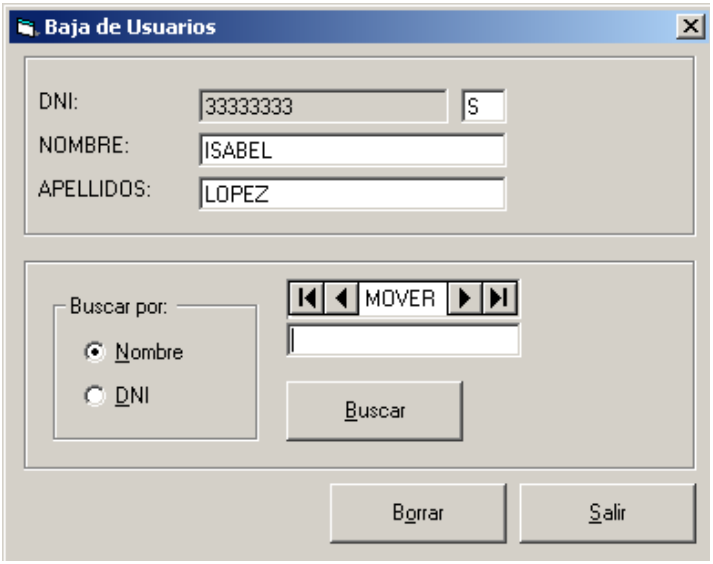


Figura 44. Ventana baja usuario.

Las funcionalidades que ofrece esta ventana son las siguientes:

1. Visualización de nombre, apellidos y DNI del registro seleccionado.
2. Desplazamiento entre registros.
3. Búsqueda por nombre o DNI.
4. Borrado de registro.
5. Salir.

El usuario administrador localizará el registro que desea borrar. Una vez verificados nombre y DNI del registro seleccionado, el administrador hará clic en el botón "Borrar".

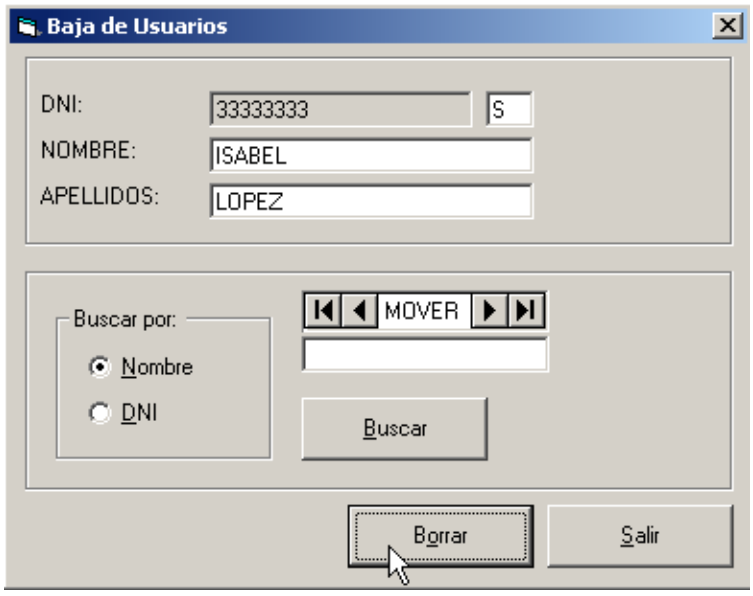


Figura 45. Borrar usuario.

Por seguridad Audit Systems antes de eliminar el registro solicitará una confirmación del borrado:

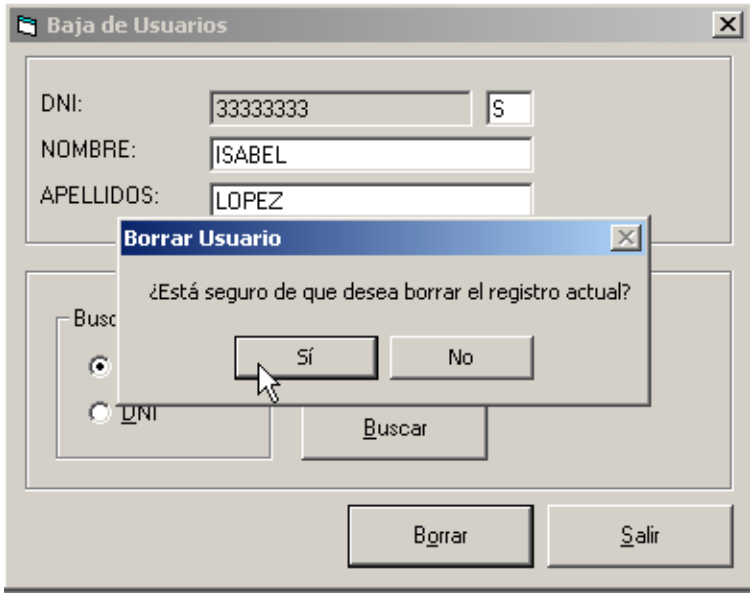


Figura 46. Confirmación de borrado registro.

Si el administrador confirma el borrado, Audit Systems eliminará el registro del usuario con todos sus datos y confirmará la eliminación mediante un mensaje. Si el administrador decide no borrarlo, el registro no será eliminado.

Las funcionalidades de desplazamiento entre registros y de búsqueda de información a través del nombre y el DNI, son similares a las explicadas en la ventana de modificación de usuarios, por lo que se remite al lector a este apartado para su consulta.

Menú Informes.

El menú "Informes", también accesible mediante el teclado "Alt + I", dispone de una única entrada: análisis.

Figura 47. Menú informes.

Bien a través de esta entrada, o bien a través del acceso "Ctrl + N", el informe final se generará automáticamente mostrando el resultado final del proceso: el informe resultante del proceso de auditoría.

Este informe contiene información confidencial sobre la empresa: procesos que es necesario mejorar, deficiencias, etc. Si bien también contempla y evalúa los procesos que se están desarrollando de forma adecuada. Esta es la razón por la cual los informes sólo se pueden generar con permisos de administrador.

Suponiendo que el lector esté leyendo este manual para aprender el uso, o bien para utilizar Audit Systems, aún no ha llegado el momento de generar los informes. La razón es simple: es necesario el procesamiento de datos previo. Téngase en cuenta que la evaluación del informe se realiza a partir de los datos recogidos por el personal de la empresa.

Es por ello que se ha adoptado la decisión de posponer la explicación sobre los informes finales hasta finalizar la fase de procesamiento de datos. Para ello se ha habilitado un nuevo capítulo, Módulo de Informes, que mostrará toda la información referente a este punto.

3.3. MÓDULO DE PROCESAMIENTO.

El módulo de procesamiento de datos es la parte de Audit Systems que se utiliza para la ejecución de los cuestionarios de evaluación de procesos, así como para recoger las respuestas a dichos cuestionarios. También es la parte que permite evaluar si los procesos que se desarrollan en la empresa auditada se están realizando de forma adecuada.

Como ya se ha explicado con anterioridad, estos cuestionarios han sido realizados con una metodología basada en los Objetivos de Control para la Información y Tecnologías Relacionadas de ISACA, así como la Guía de Seguridad de SEDISI y se han cubierto los cuestionarios MARION.

Se trata por tanto de la parte más importante de la aplicación, dado que es la que aplica la metodología de forma operativa y sencilla a los procesos. Es por ello que los cuestionarios han sido tratados en su propio capítulo, Cuestionarios, al cual remitimos al lector si desea encontrar más información al respecto.

Es necesario tener en cuenta que la información contenida en este módulo es variable. El diseño de la parte de procesamiento de Audit Systems permite que los cuestionarios varíen a lo largo del tiempo, permite la inclusión, actualización y borrado de datos.

Así pues si en un futuro varía la normativa aplicable, o bien si se desean cargar nuevos cuestionarios, bastará con introducir la información conveniente en la base de datos. Audit Systems no sufrirá cambios.

El módulo de procesamiento requiere del alta previa de usuarios en el módulo de administración. El proceso previsto es el siguiente:

1. Existe una empresa que será auditada.

2. El auditor experto decide qué personas de esta empresa deben responder a los cuestionarios para la recogida de datos.

3. Las personas son dadas de alta en el sistema. A cada una de ellas se le ofrecerá un usuario de acceso y una clave.

4. Cada persona se conectará a la Terminal de Audit Systems que se situará en la empresa auditada, e introducirá las respuestas a las preguntas que se le planteen.

Las entradas y salidas que ofrece este módulo de Audit Systems son las siguientes:

Figura 48. Entradas y salidas módulo procesamiento.

Audit Systems presenta una serie de ventajas:

- Se tratará de un ordenador habilitado en la empresa, por lo que el personal seleccionado no tendrá que desplazarse.

- Cabe destacar también que al tratarse de un ordenador no es necesario tomar cita previa. Los trabajadores de la empresa auditada podrán buscar los momentos en que se encuentren menos atareados para responder a las preguntas.

- Audit Systems está diseñada de tal forma que permite detener y continuar el proceso en cualquier momento. Así por ejemplo si un trabajador estuviese contestando a los cuestionarios y de repente surgiese una urgencia que requiera su presencia, podrá salir de la aplicación y en el siguiente acceso seguirá exactamente en la cuestión en que se encontraba cuando cerró la aplicación.

Lógicamente no todo son ventajas:

- Se trata de una aplicación y como tal no es capaz de evaluar la veracidad de las respuestas. Si bien las personas tampoco tenemos esta capacidad, sí somos más intuitivas y digamos que resulta más sencillo obtener respuestas más precisas.

- Por otro lado si bien Audit Systems realiza distintas preguntas en función del perfil que tenga asociado el usuario al que se plantean las cuestiones, no es capaz de elaborar nuevas preguntas en función de las respuestas previas del empleado.

Aún así, indiscutiblemente, Audit Systems supone una excelente ayuda al auditor experto.

A continuación se explicará cómo se usa el módulo de procesamiento de datos de Audit Systems.

EJECUCIÓN MÓDULO DE PROCESAMIENTO

Es suficiente con acceder a la aplicación con un usuario que no sea del tipo administrador.

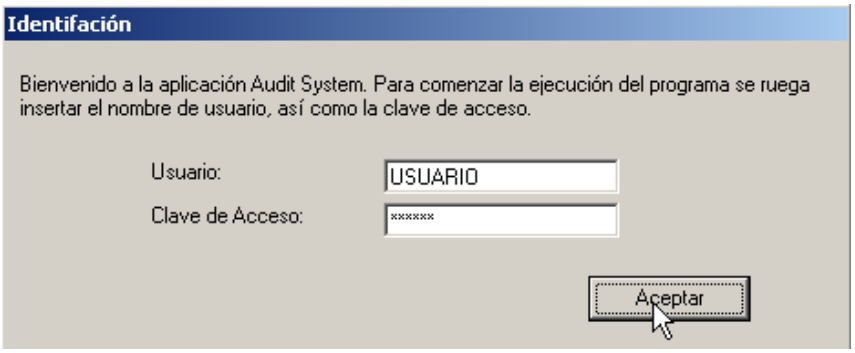


Figura 49. Ventana de identificación.

Si el usuario y la contraseña son correctos, se accederá al módulo de procesamiento. Se mostrará entonces una ventana de información:

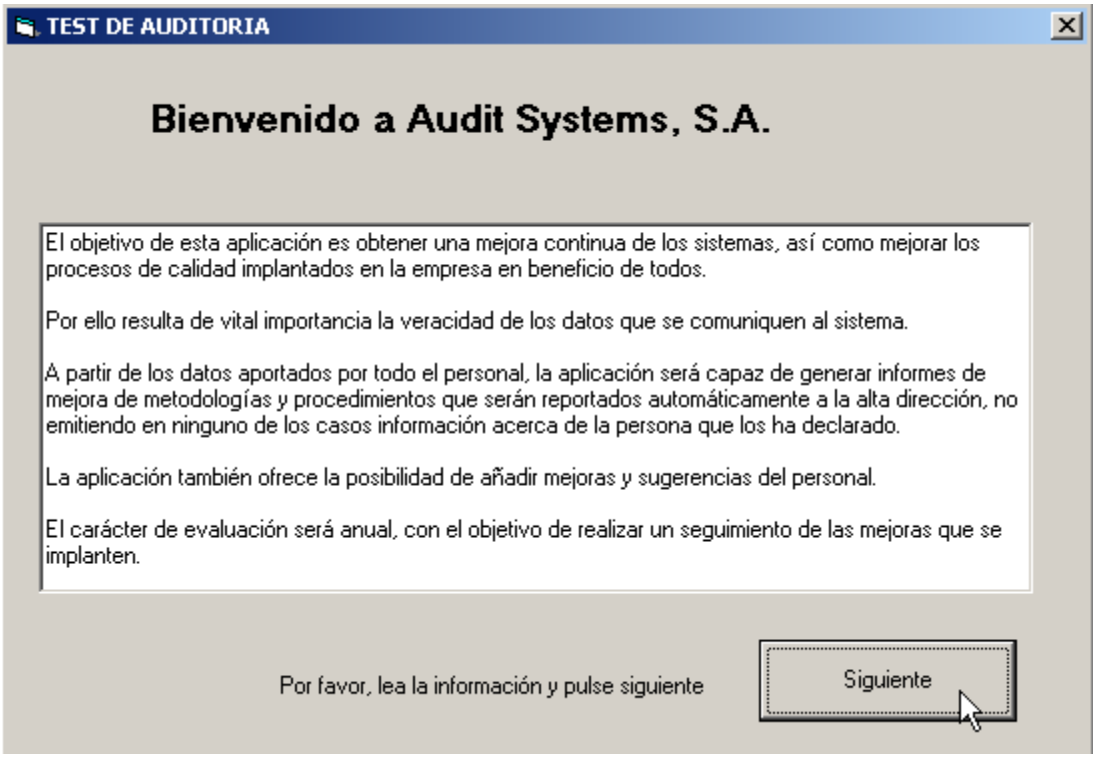


Figura 50. Ventana acceso.

Se hará clic en el botón siguiente. Aparecerá entonces la primera ventana con preguntas:

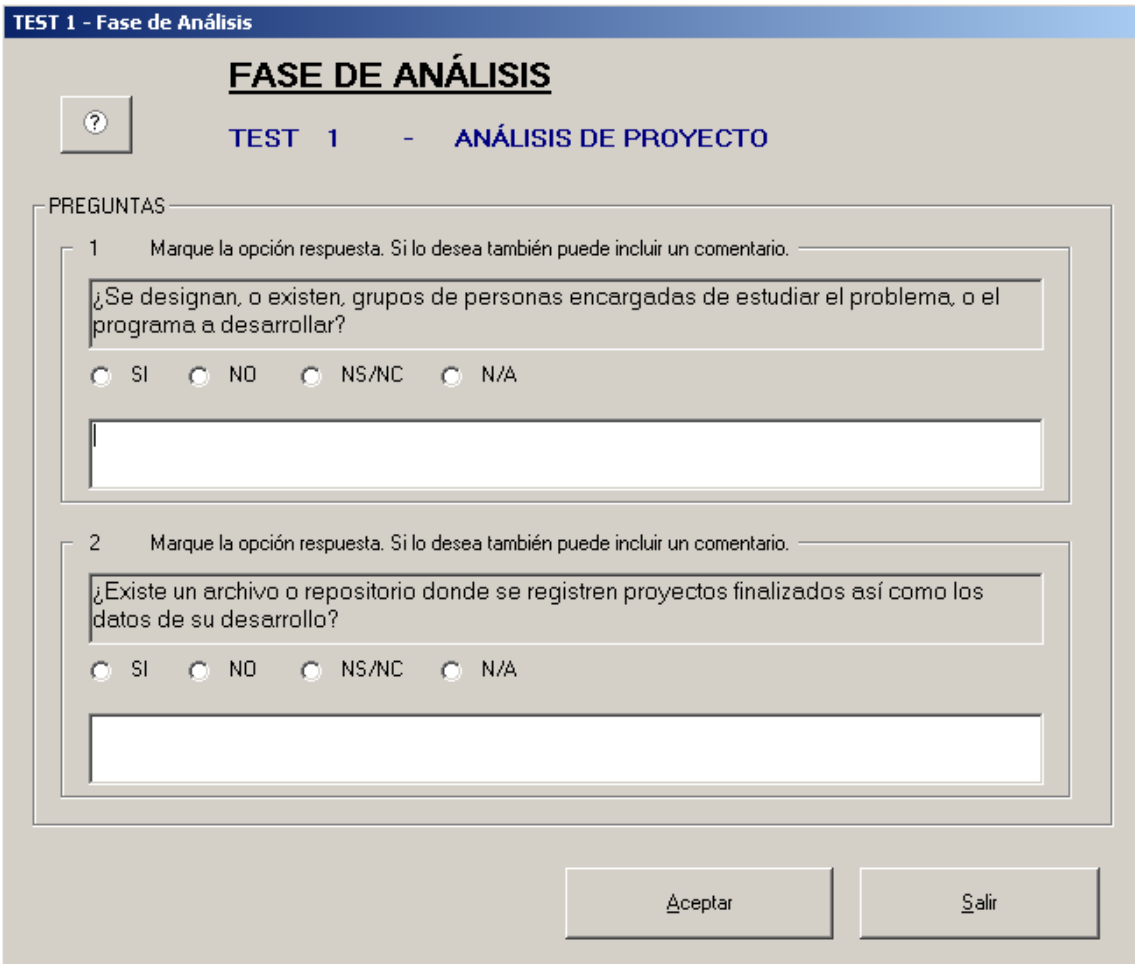


Figura 51. Ventana cuestionario.

El usuario deberá leer las preguntas de una en una e irlas contestando. Para ello se ayudará de las opciones de respuesta de la aplicación:

- Si.
- No.
- NS/NC: No sabe, no contesta.
- N/A: No aplicable.

Tendrá ocasión de introducir un comentario a cualquier pregunta siempre y cuando lo considere necesario. Para ello utilizará el espacio habilitado debajo de cada pregunta.

En cualquier momento el usuario podrá hacer clic en el botón de ayuda si le surge alguna duda.

Figura 52. Ayuda.

Este icono se encuentra en la parte superior izquierda de todas las ventanas cuestionario. Al presionarlo se mostrará una ventana de ayuda recordando el significado de cada opción.

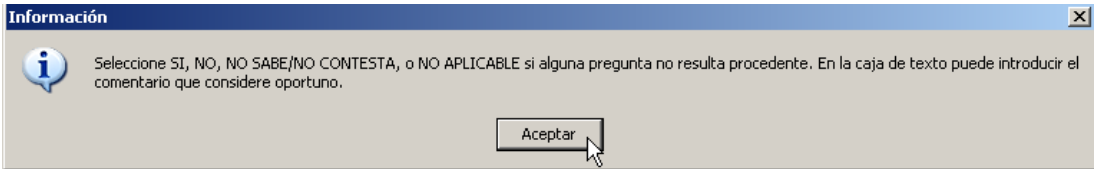


Figura 53. Resultado de la ayuda.

Cuando el usuario esté listo para responder las preguntas podrá comenzar a hacerlo. Todas las preguntas de los cuestionarios deberán ser contestadas.

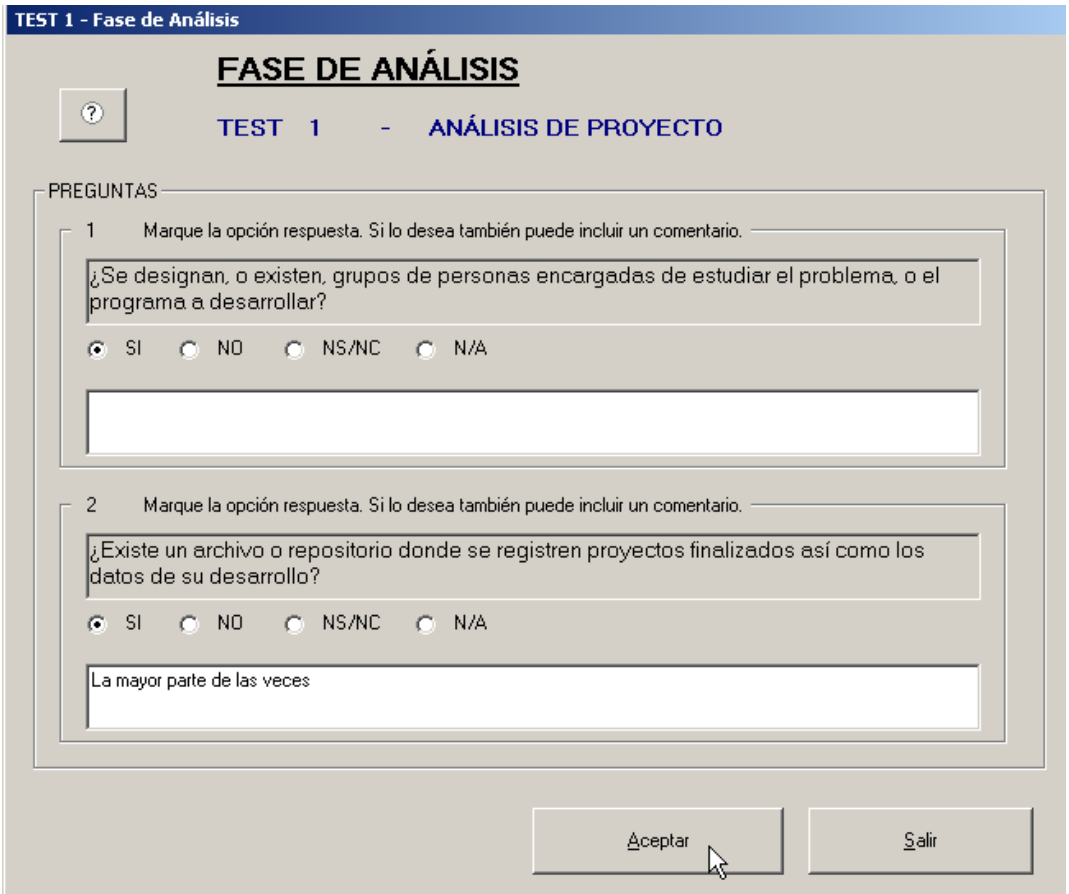


Figura 54. Cuestionario contestado.

Como puede observarse en el ejemplo que se muestra, el usuario ha respondido las preguntas 1 y 2, del Cuestionario 1 de Análisis de Proyecto. En la pregunta 2 ha considerado necesario incluir un comentario.

Para pasar a la siguiente ventana y grabar la información que se ha introducido, se hará clic en el botón "Aceptar", o bien se utilizará el teclado "Alt + A".

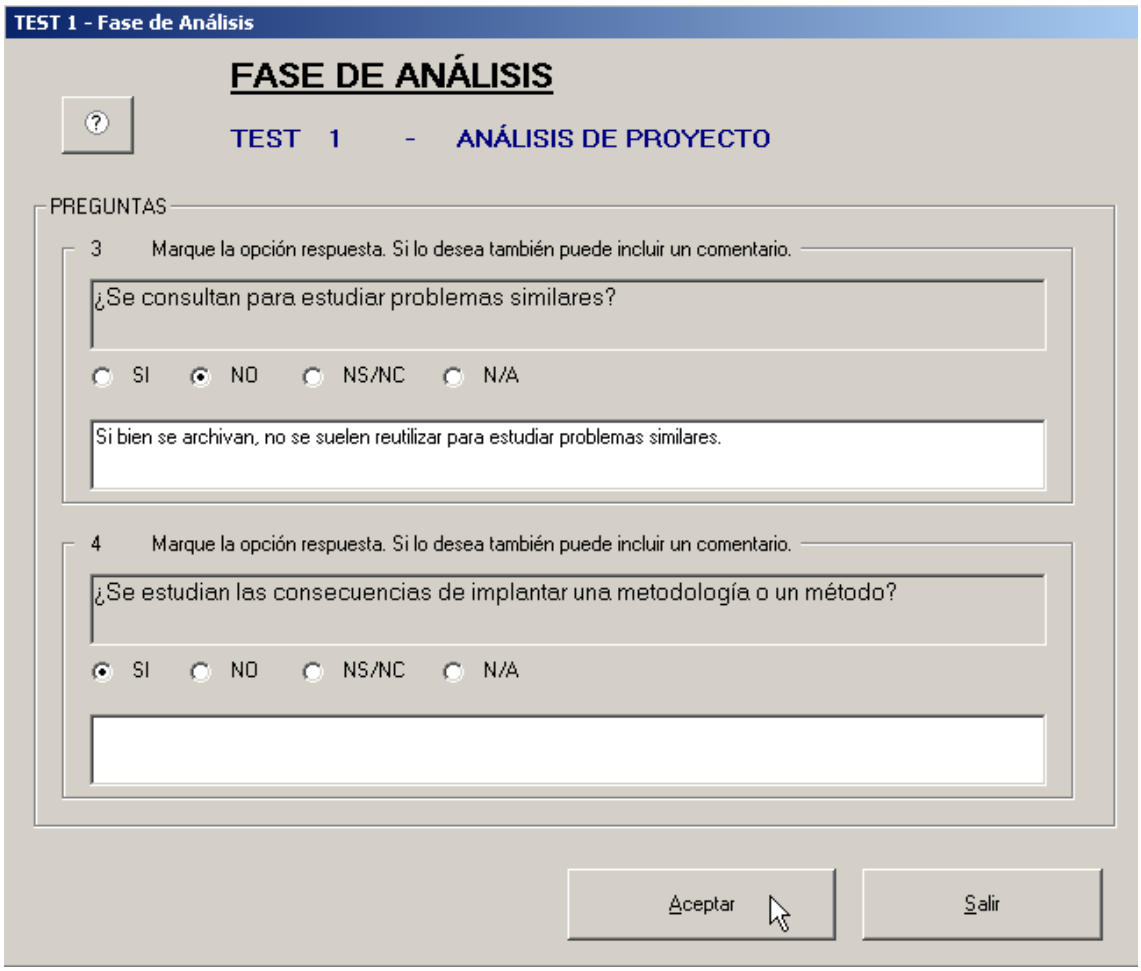


Figura 55. Siguiente cuestionario.

De nuevo el usuario podrá repetir el proceso contestando a las nuevas preguntas y haciendo clic en el botón "Aceptar" para pasar a la siguiente ventana.

El proceso para contestar todas las preguntas es el mismo y se repite una y otra vez hasta que el usuario haya contestado a todos los cuestionarios que le afecten, en función del puesto de trabajo que desempeñe.

Como ya se dijo anteriormente, si el usuario lo desea podrá interrumpir el proceso de preguntas-respuestas para continuar haciéndolo en otro momento.

Para ello bastará con hacer clic en el botón “Salir”.

Figura 56. Salir de la aplicación.

Audit Systems guarda el registro de las preguntas contestadas y es capaz de buscar la pregunta que corresponde responder a cada usuario.

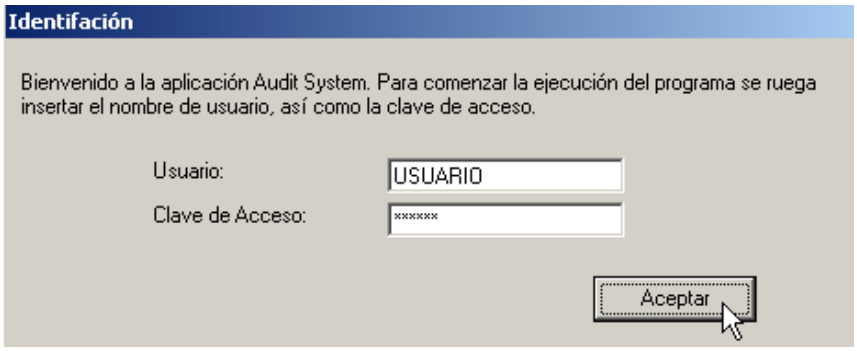


Figura 57. Ventana de acceso.

Por ello cuando el mismo usuario acceda de nuevo a la aplicación, se mostrará la siguiente pregunta que tuviese pendiente de contestación.

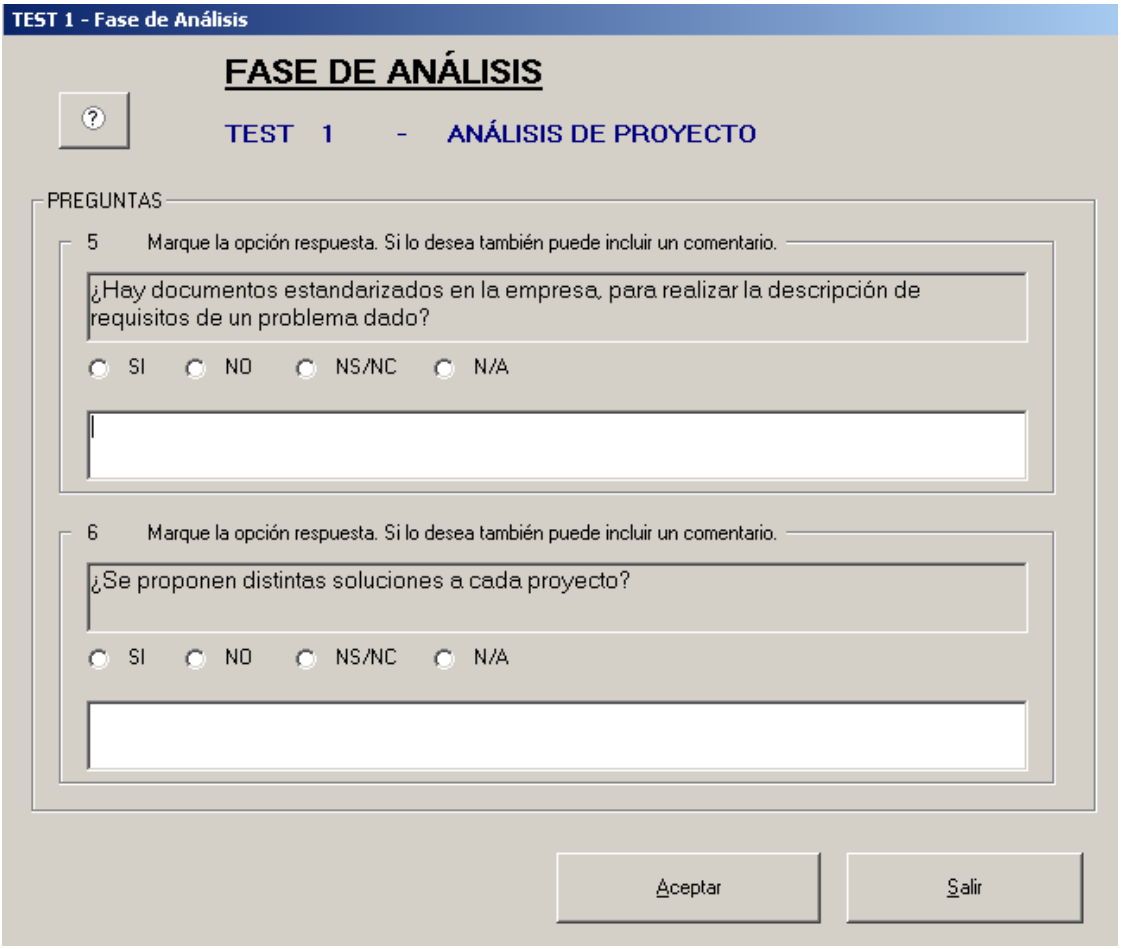


Figura 58. Búsqueda automática cuestionario.

Recuérdese que el usuario había contestado hasta la pregunta 4 del cuestionario 1. Por ello al conectarse de nuevo se muestra el la pregunta 5 del mismo cuestionario.

Sin embargo al acceder con un usuario distinto se mostrarán las cuestiones y respuestas del nuevo usuario.

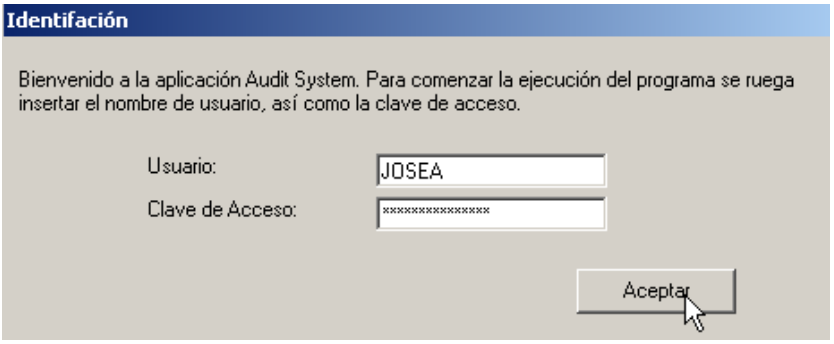


Figura 59. Acceso de un nuevo usuario.

En esta ocasión se muestra el ejemplo en que se conecta un nuevo usuario, Jose Antonio, con el mismo perfil pero más avanzado en sus respuestas. Por tanto visualiza una pantalla más avanzada, pregunta 1 del Cuestionario 6.

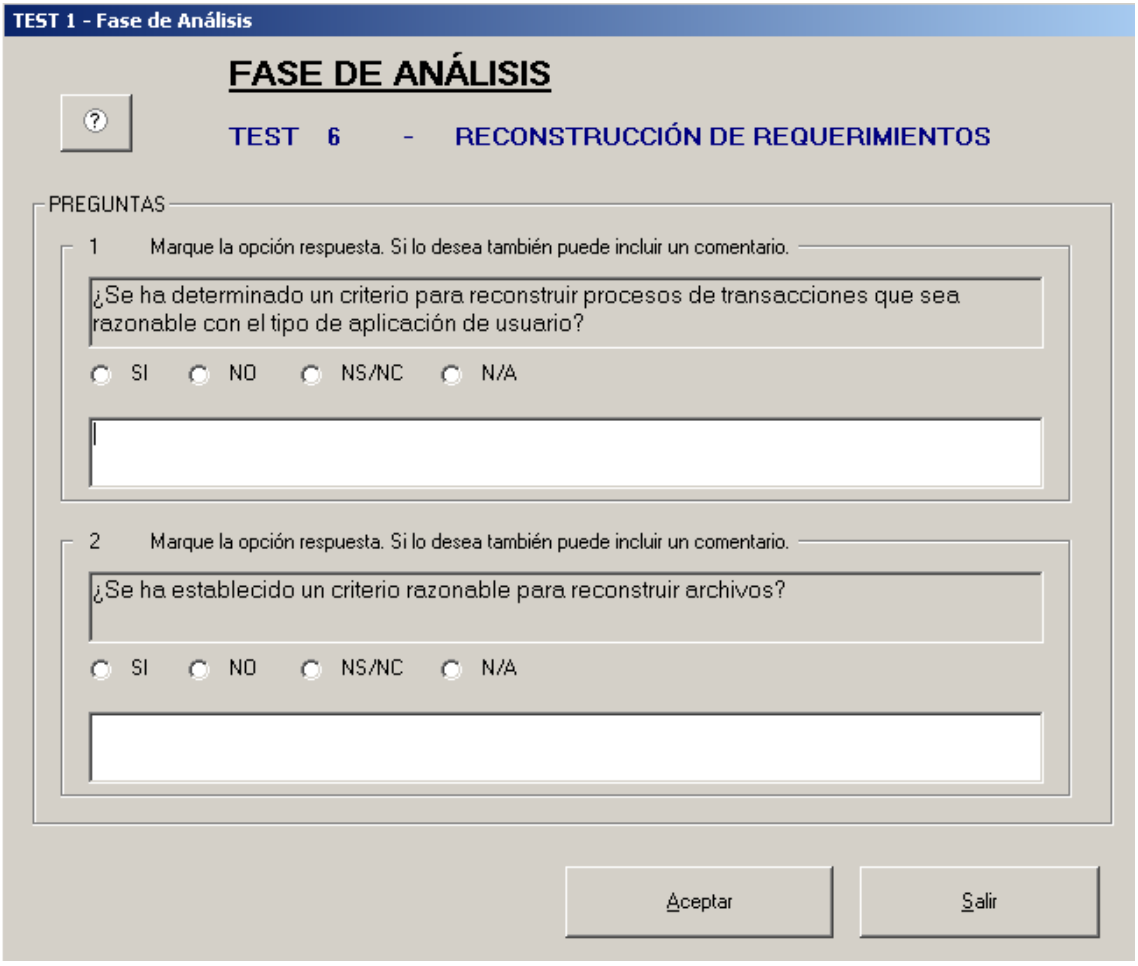


Figura 60. Búsqueda de cuestionario para nuevo usuario.

Audit Systems gestiona la concurrencia entre usuarios, por lo que disponiendo de distintas máquinas los distintos usuarios podrán responder cada uno a sus preguntas en el mismo momento de tiempo.

Por otro lado reseñar que Audit Systems no permite editar las contestaciones que se han dado con anterioridad. En la fase de análisis y diseño se concluyó que sería la mejor forma de hacerlo.

El objetivo que se persigue es que el usuario no pueda realizar rectificaciones posteriores para cuadrar la información con las respuestas que esté dando a las nuevas preguntas.

Es preferible que el auditor externo al notar la discordancia en los informes generados, averigüe personalmente a qué se debe la diferencia entre las respuestas y profundice en lo que esté ocurriendo.

3.4. MÓDULO DE INFORMES.

Tal y como se explicó en anteriores capítulos, la generación de los informes de salida requiere de las respuestas ofrecidas por el personal de la empresa auditada. Una vez procesadas las respuestas en el sistema, será posible generar el informe de auditoría.

El informe de auditoría que genera Audit Systems es un informe con formato habitual, que contiene los siguientes apartados:

1. Introducción al informe de auditoría.
   - **a. Fase de análisis.**
     - i. Introducción a la auditoría en la fase de análisis.
       1) Informe-Evaluación del Test 1 de la fase de análisis.
          - I. Resumen de puntos incorrectos y soluciones recomendadas.
            a) Punto incorrecto 1 + Recomendación 1.
            b) Punto incorrecto 2 + Recomendación 2.
            c) …
            d) Otras recomendaciones.
            e) …
       2) Informe-Evaluación del Test 2 de la fase de análisis.
          - I. Resumen de puntos incorrectos y soluciones recomendadas.
            f) Punto incorrecto 1 + Recomendación 1.
            g) …
            h) Otras recomendaciones.
            i) …
       3) Informe-Evaluación del Test 3 de la fase de análisis....
   - **b. Fase de diseño.**
     - i. Introducción a la auditoría en la fase de diseño.
       1) Informe-Evaluación del Test 1 de la fase de diseño.
          - I. Resumen de puntos incorrectos y soluciones recomendadas.
            j) Punto incorrecto 1 + Recomendación 1…
            k) Otras recomendaciones…
       2) Informe-Evaluación del Test 2 de la fase de diseño...
   - **c. Fase de desarrollo...**

Es decir primeramente se muestra una introducción al informe de auditoría. El informe se divide en distintos capítulos, en función de la fase del proyecto que se esté tratando: análisis, diseño, desarrollo…

Para cada uno de los capítulos-fases de proyecto, se realiza una introducción a la fase y lo que se debe revisar en el proceso de auditoría.

Dentro de esa fase **se evalúa el resultado de las respuestas ofrecidas** a cada cuestionario. Se genera un apartado-informe para cada uno de los cuestionarios realizados, dado que contemplan distintos puntos a evaluar.

La información que se muestra en el informe se genera de forma priorizada. Es decir los asuntos más importantes y que se estén desarrollando de forma inadecuada se colocarán siempre en primer lugar.

La ordenación se ha logrado gracias a distintos **grados de importancia o pesos**, que se han asignado a cada una de las preguntas.

Por último **al final de cada informe - cuestionario** se realiza automáticamente un **resumen del texto**, también de **forma priorizada**, haciendo constar:

- Los **puntos más graves incorrectos** que se deben solventar a la mayor brevedad, **junto a la recomendación propuesta** para solventarlos.

- **Recomendaciones varias** a comprobar en la empresa, ya menos importantes.

Como puede observarse a lo largo de esta explicación, en el módulo de informes se ha conseguido generar información automática priorizada, junto a recomendaciones precisas para cada proceso que no se está realizando bien. Es más, se ha conseguido mostrar la información de forma coherente y sin dejar espacios en blanco, ajustando exactamente el resultado del informe a las conclusiones previstas.

A continuación se explicará cómo generar el informe:

Recuérdese que la generación del informe de auditoría requiere el acceso a Audit Systems con permisos de administrador.

Para generar el informe de auditoría será necesario seleccionar el menú “Informes”, también accesible mediante el teclado “Alt + I”.

Figura 61. Informe análisis.

Se seleccionará entonces la única entrada que tiene, “Análisis”, o bien se accederá mediante el teclado “Ctrl + N”.

Al hacerlo automáticamente se generará el informe de auditoría. Comprobemos como se muestran los apartados descritos con anterioridad:

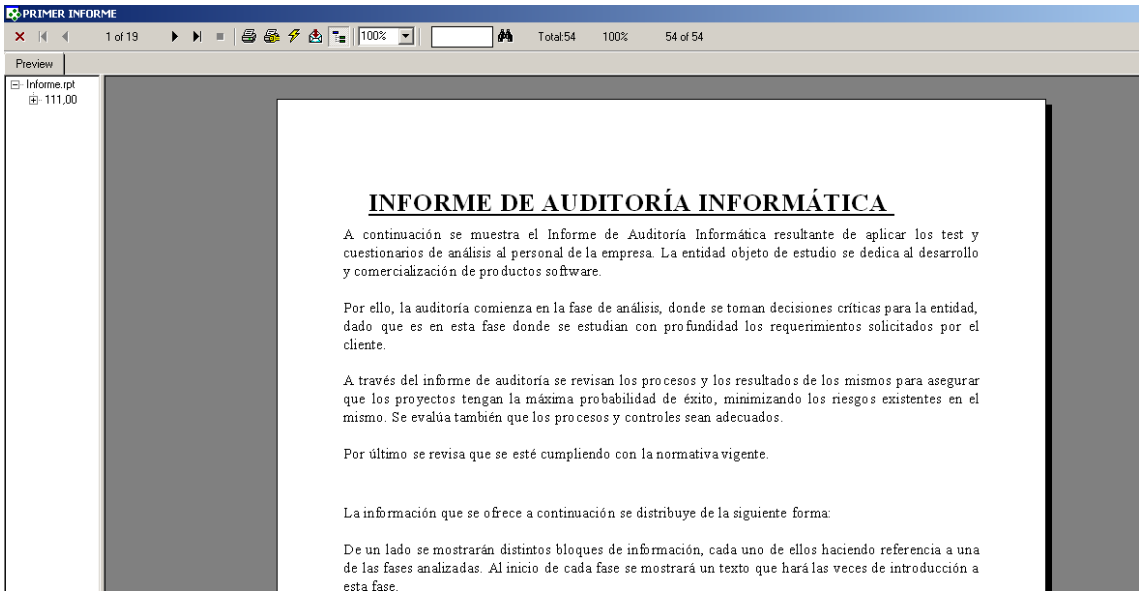


Figura 62. Informe auditoría.

La primera imagen muestra efectivamente la introducción al informe de auditoría.

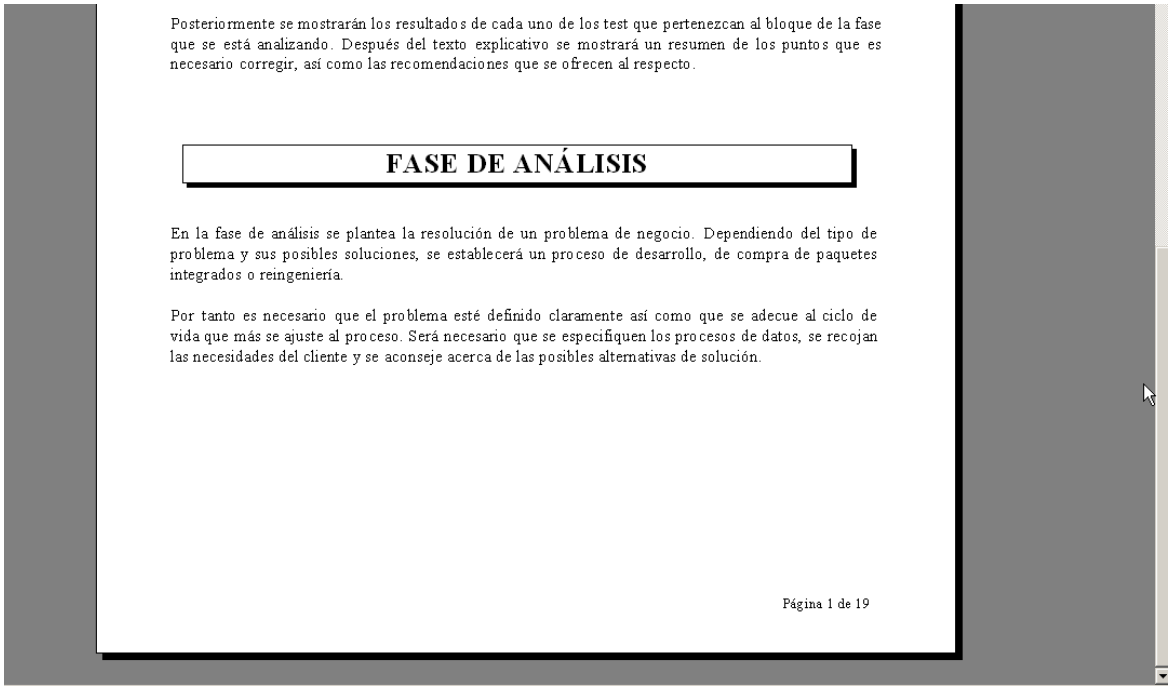


Figura 63.Pie informe auditoría.

Como muestra la imagen anterior, desplazando la barra de herramientas se alcanza la parte inferior de la hoja, donde se puede comprobar que efectivamente está la fase de análisis junto a su introducción.

Nótese también que el informe está numerado. Concretamente en la imagen se está visualizando la hoja 1 de 19 totales.

Por otro lado si el usuario administrador desea ver la hoja al completo, podrá seleccionar la opción de visualización que permite ajustar el tamaño.

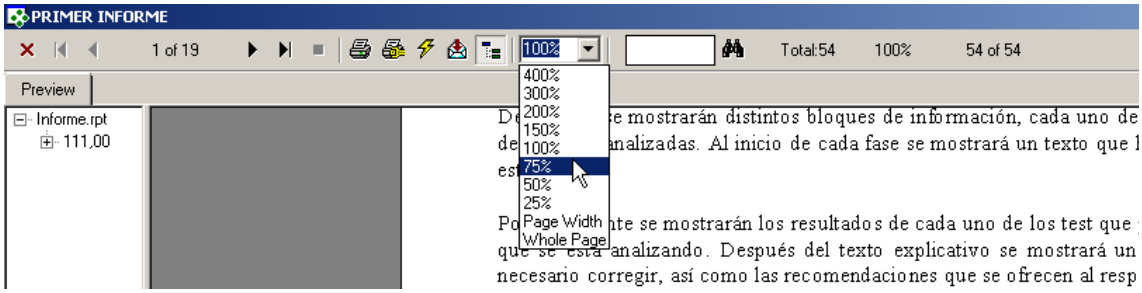


Figura 64.Resolución informe.

De forma inmediata la hoja adquirirá el tamaño requerido.

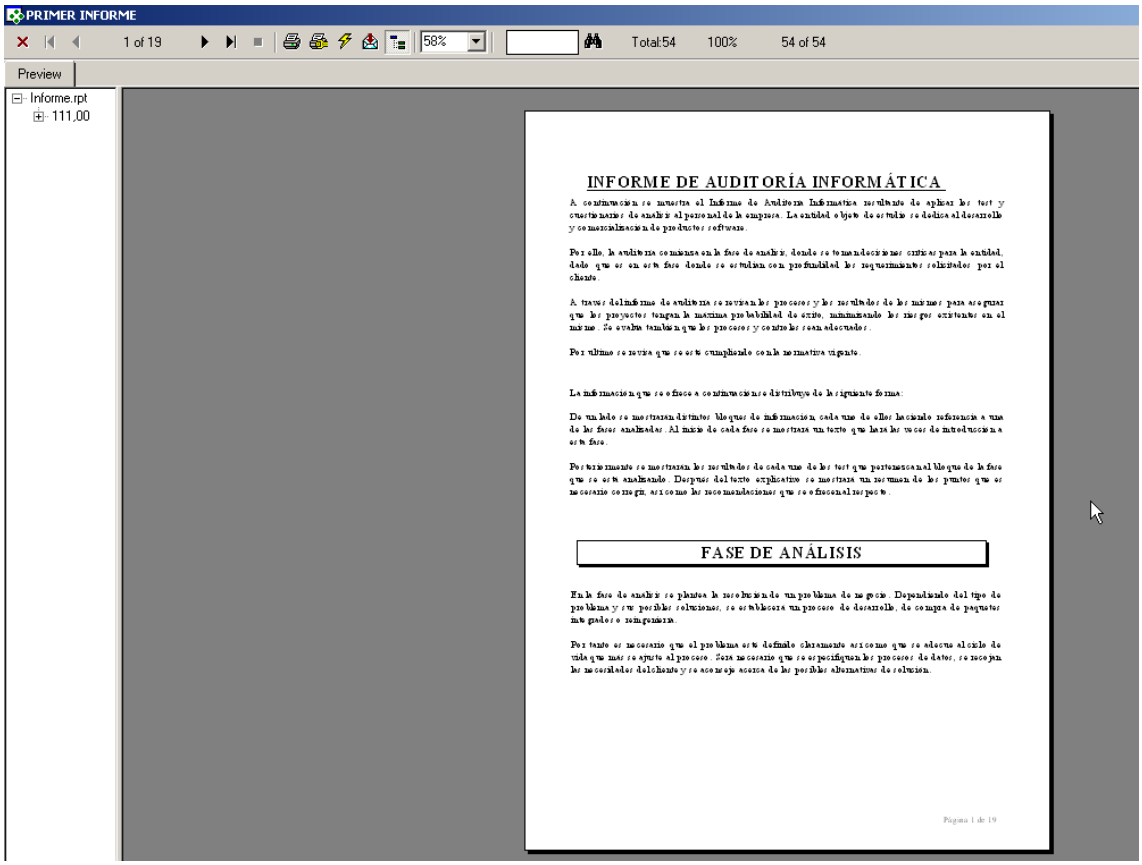


Figura 65.Resultado resolución informe.

Para continuar comprobando la información que se muestra el usuario administrador podrá utilizar las flechas de posicionamiento, a fin de desplazarse a la siguiente hoja.

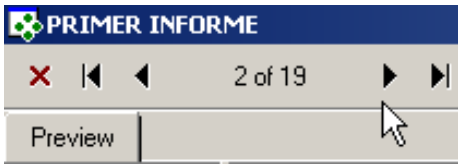
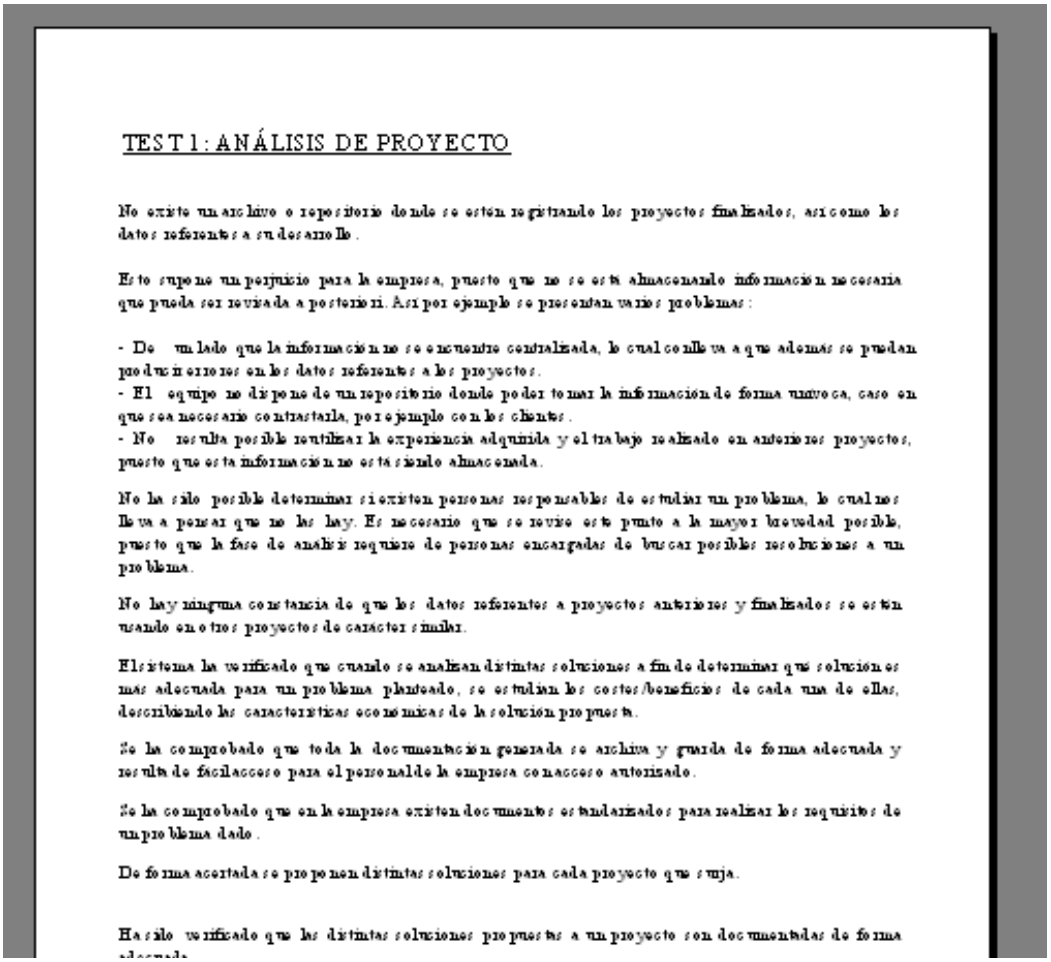


Figura 66. Desplazamiento informe.

De izquierda a derecha el funcionamiento es el siguiente:

- La cruz se usa para cerrar el informe, regresando a la parte administradora de Audit Systems.
- La flecha situada a continuación permite situarse en la primera hoja del informe.
- La siguiente flecha permite situarse en la hoja previa del informe.
- La siguiente visualizaría la hoja siguiente.
- Y la última mostraría la última hoja del informe.

Como puede observarse en el centro se indica el número de página que se está visualizando con respecto al total. Una vez dicho lo anterior, se comprueba que efectivamente la hoja 2 incluye el informe de evaluación del primer test de la fase de análisis.



TEST 1: ANÁLISIS DE PROYECTO

No existe un archivo o repositorio donde se estén registrando los proyectos finalizados, así como los datos referentes a su desarrollo.

Esto supone un perjuicio para la empresa, puesto que no se está almacenando información necesaria que pueda ser revisada a posteriori. Así por ejemplo se presentan varios problemas:

- De un lado que la información no se encuentre centralizada, lo cual conlleva a que además se puedan producir errores en los datos referentes a los proyectos.
- El equipo no dispone de un repositorio donde poder tomar la información de forma unívoca, caso en que sea necesario contrastarla, por ejemplo con los clientes.
- No resulta posible rentabilizar la experiencia adquirida y el trabajo realizado en anteriores proyectos, puesto que esta información no está siendo almacenada.

No la sido posible determinar si existen personas responsables de estudiar un problema, lo cual nos lleva a pensar que no las hay. Es necesario que se revise este punto a la mayor brevedad posible, puesto que la fase de análisis requiere de personas encargadas de buscar posibles resoluciones a un problema.

No hay ninguna constancia de que los datos referentes a proyectos anteriores y finalizados se estén usando en otros proyectos de carácter similar.

El sistema ha verificado que cuando se analizan distintas soluciones a fin de determinar qué solución es más adecuada para un problema planteado, se estudian los costes/beneficios de cada una de ellas, describiendo las características económicas de la solución propuesta.

No ha comprobado que toda la documentación generada se archiva y guarda de forma adecuada y resulta de fácil acceso para el personal de la empresa con acceso autorizado.

No ha comprobado que en la empresa existen documentos estandarizados para realizar los requisitos de un problema dado.

De forma acertada se proponen distintas soluciones para cada proyecto que surja.

Ha sido verificado que las distintas soluciones propuestas a un proyecto son documentadas de forma

Figura 67.Segunda hoja.

A continuación de este informe evaluación, según el esquema inicial, se muestran los puntos a corregir, cada uno junto a su recomendación.

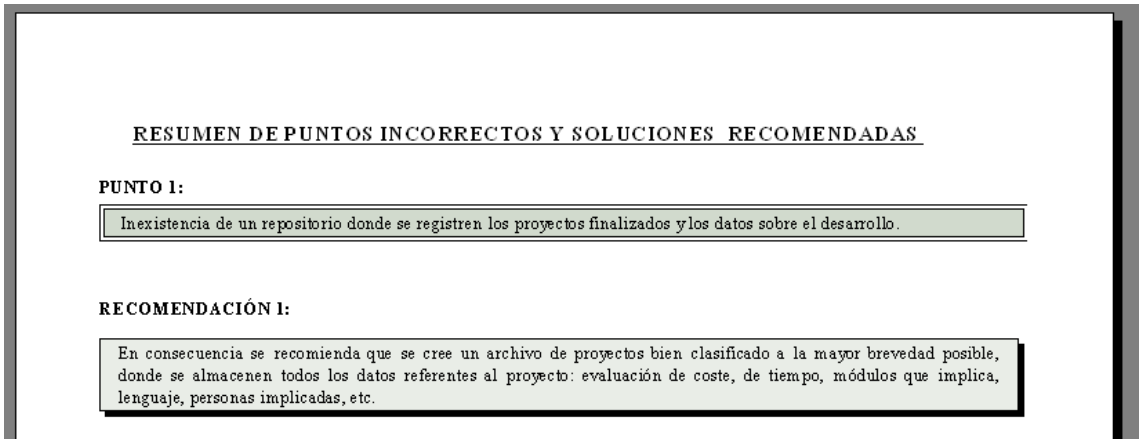


Figura 68. Puntos a corregir.

Y finalmente se muestran otras recomendaciones menos importantes:

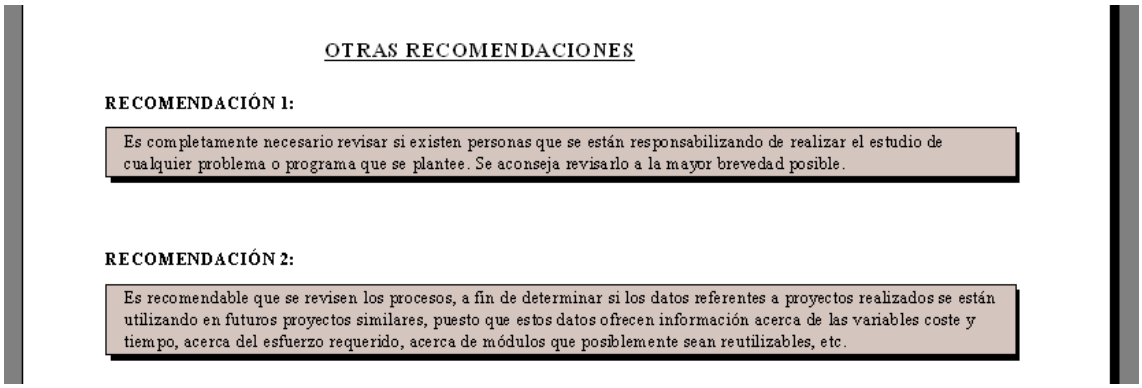


Figura 69. Recomendaciones.

A continuación se muestra el siguiente informe, elaborado sobre el siguiente cuestionario de la fase de análisis. Al final del mismo se añadirá un nuevo resumen de los puntos a corregir y las recomendaciones para cada punto, así como recomendaciones generales.

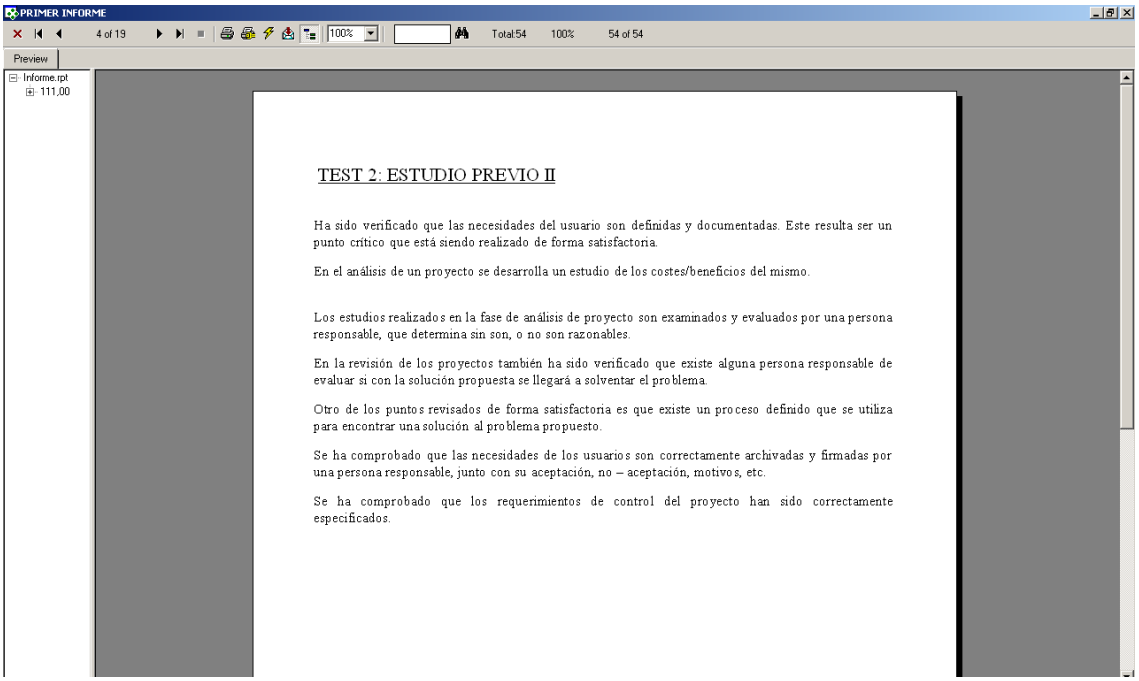


Figura 70. Siguiente informe.

Una vez finalizado ese informe se pasará al siguiente, hasta que todos los cuestionarios de la fase de análisis hayan sido generados y se pase a la siguiente fase, diseño, etc. repitiendo el mismo proceso en todos sus cuestionarios.

Puesto que ya se ha verificado cómo se está generando la estructura del informe, a continuación el lector ya está preparado para comprender la estructura de árbol de información que se muestra en Audit Systems.

Nótese que en la parte izquierda de la ventana se muestra un margen en blanco.

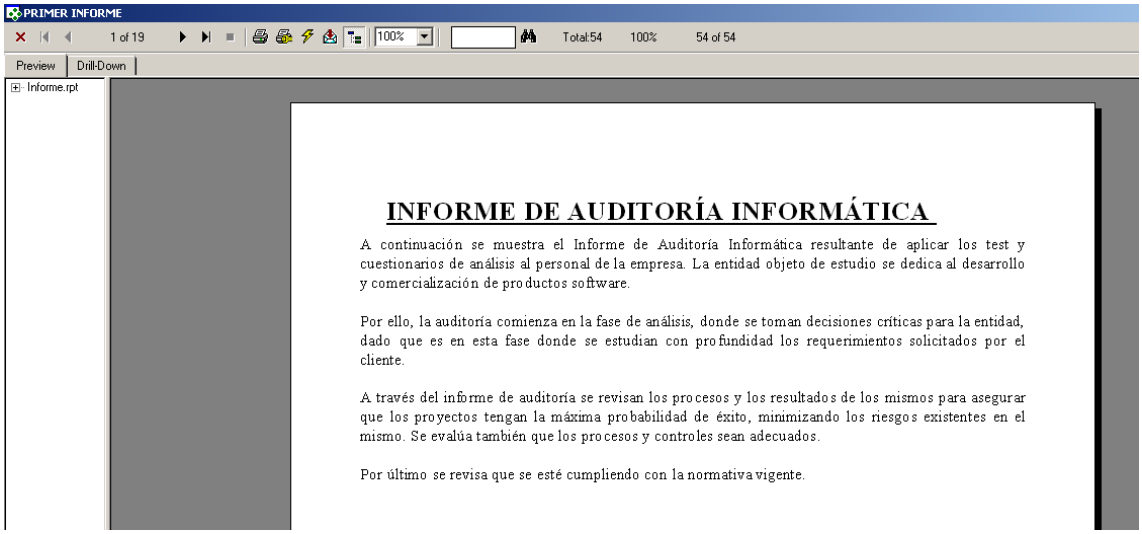


Figura 71. Margen izquierdo.

Si el margen no se mostrase es necesario activarlo, usando el siguiente icono, que también sirve para desactivarlo después:

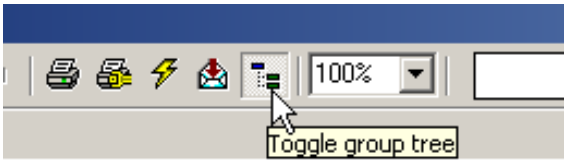


Figura 72. Activar margen izquierdo.

Ese margen contiene una estructura de acceso a la información. Para agrandar el margen se podrá usar el ratón, situándolo en el borde del margen y arrastrándolo en la dirección que se precise manteniendo presionado el botón del ratón.

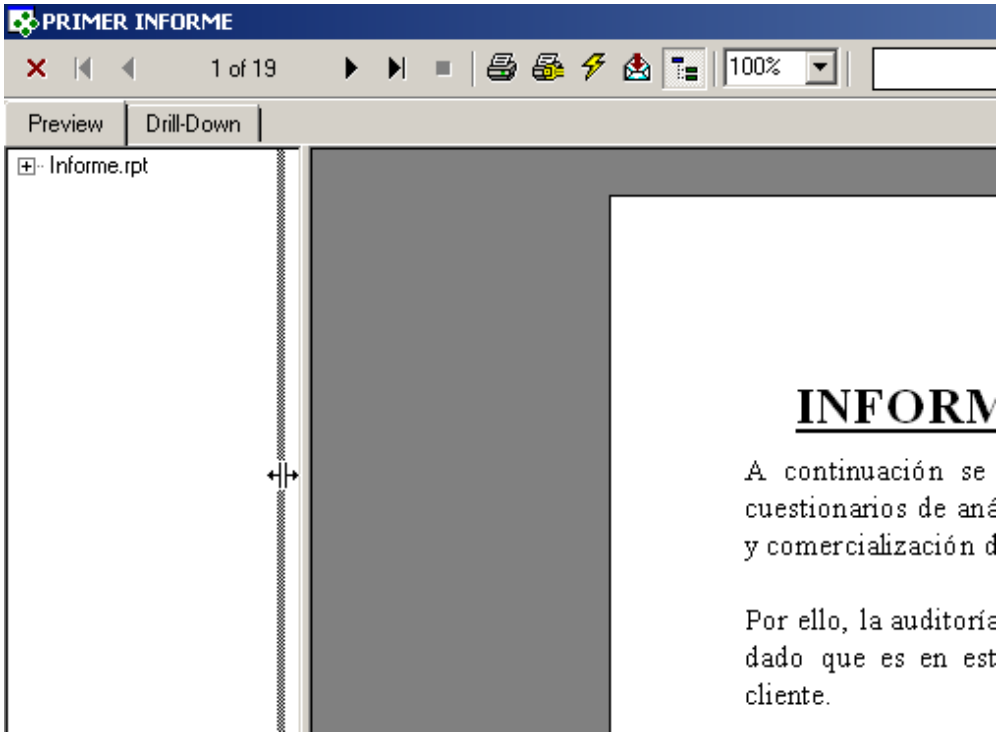


Figura 73. Desplazar margen izquierdo.

Para revisar la información que contiene será preciso hacer el margen más ancho como muestra la imagen anterior. A continuación se desplegará el árbol, cuya raíz es "Informe.". Para ello se hará clic en el símbolo "+" situado a la izquierda de "Informe".

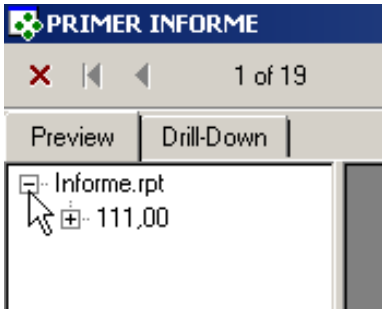


Figura 74. Desplegar información.

Se muestra "111". Ese primer número, independientemente de cual sea, es el identificador de un empleado que ha contestado ciertos cuestionarios. A continuación se despliega de la misma forma la información que contiene:

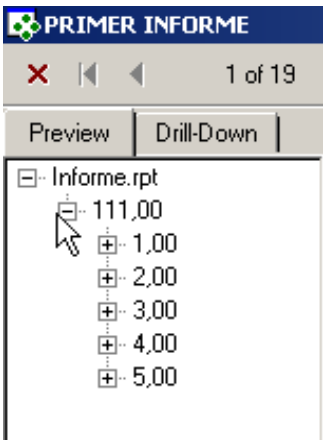


Figura 75. Desplegar cuestionarios.

La nueva información que se muestra se corresponde con los cuestionarios que han sido contestados por el usuario. El administrador, haciendo clic en cada uno de estos cuestionarios, se podrá desplazar automáticamente al cuestionario seleccionado.

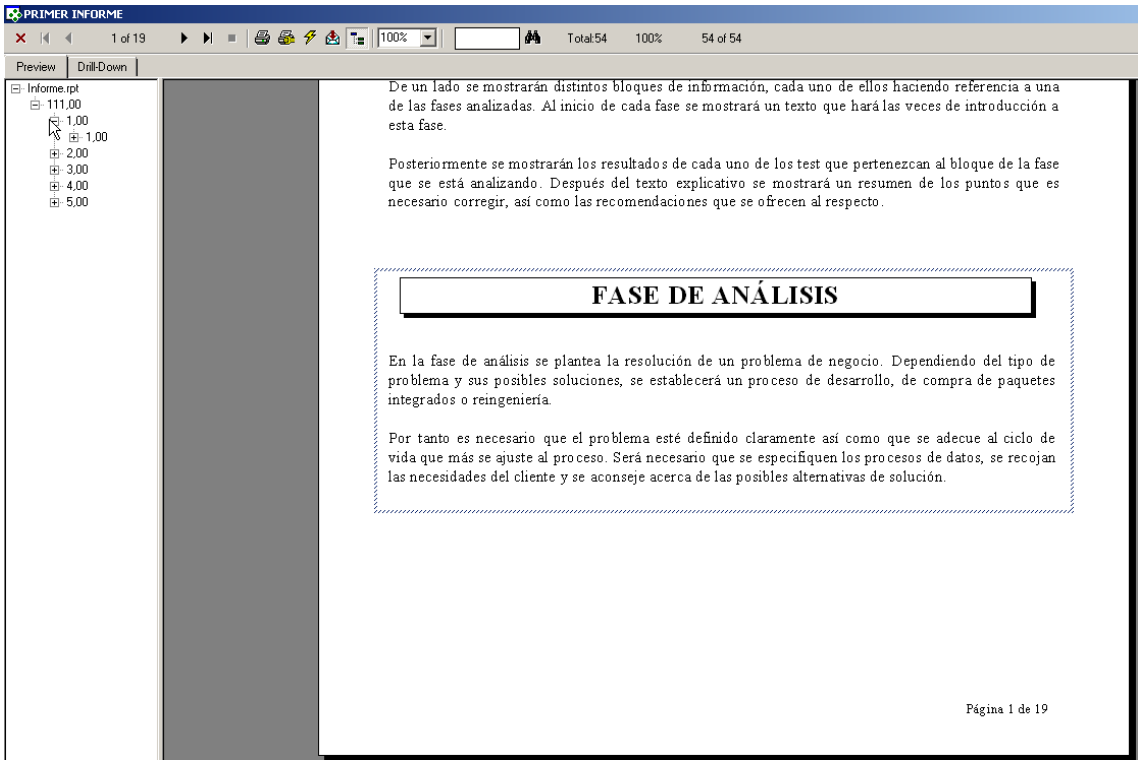


Figura 76. Desplazarse a cuestionario.

Así por ejemplo al hacer clic sobre el cuestionario 1, este se despliega y nos lleva al inicio de la fase de análisis, que es donde comienza el primer cuestionario, tal y como puede observarse en la hoja siguiente.

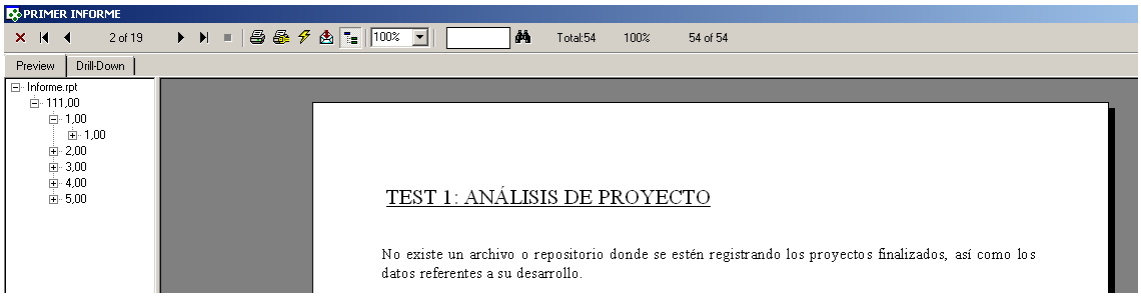


Figura 77. Desplazamiento a fase de análisis.

Si por el contrario se realiza clic en el cuestionario 3, se comprueba que el desplazamiento se realiza de igual forma, sólo que en esta ocasión hacia el cuestionario 3.

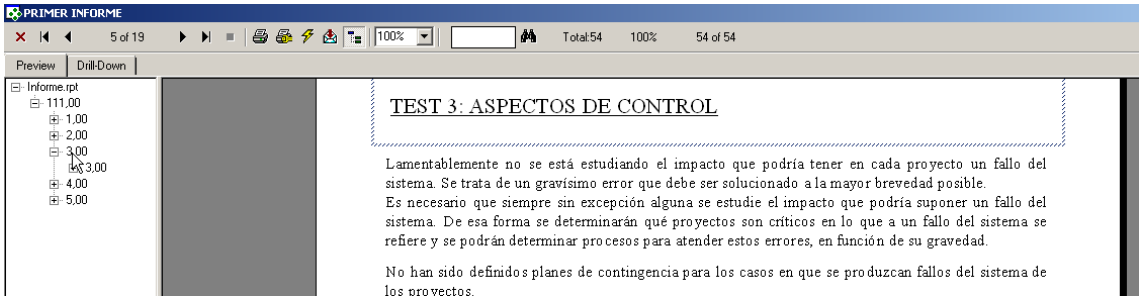


Figura 78. Desplazamiento a cuestionario 3.

Es decir seleccionando el número de cuestionario el usuario administrador se situará siempre, o bien donde comienza el cuestionario, o bien en el apartado inmediatamente anterior.

También existe la posibilidad de desplegar el cuestionario. En ese caso se mostrará información sobre qué respuestas son las que se han dado a cada cuestionario.

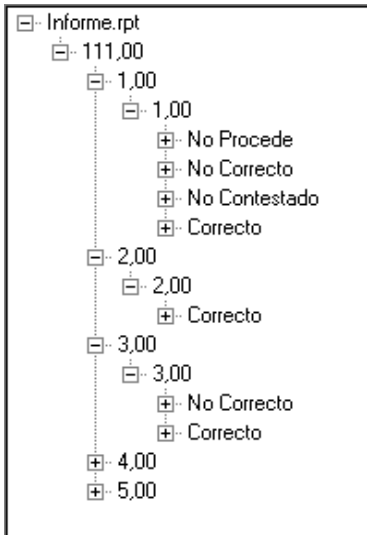


Figura 79. Desplegar cuestionario.

Así por ejemplo en el cuestionario 1 se han respondido 4 tipos de respuestas: no procede, no correcto, no contestado y correcto. Sin embargo en el cuestionario 3 sólo se dieron dos tipos de respuesta: no correcto y correcto.

El árbol está mostrando una clasificación interna que se ha realizado en los informes, a partir de la evaluación realizada sobre las respuestas. Esta clasificación es la que permite ordenar el contenido del informe, tanto en la parte desarrollada en el texto, como en los puntos resúmenes de cada capítulo.

Si el usuario administrador lo desea podrá hacer clic en las opciones de los informes. Al hacer clic sobre ellas se situará directamente en la parte de información elaborada sobre preguntas que han sido contestadas con esa opción.

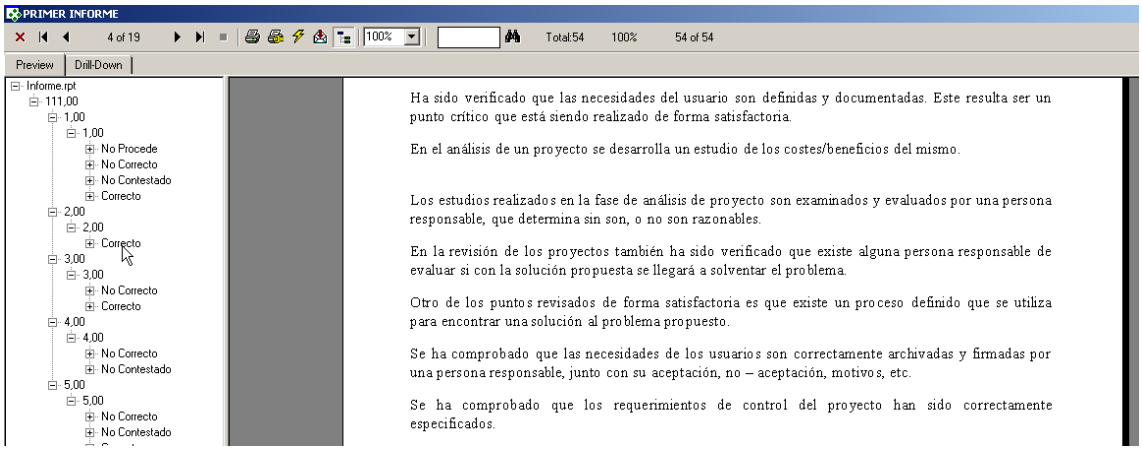


Figura 80. Desplazarse por contestaciones.

En el ejemplo descrito se ha hecho clic sobre correcto. Por tanto en este ejemplo se muestra la información elaborada a partir de las preguntas del cuestionario 2 que han sido respondidas de forma correcta:

Los estudios realizados en la fase de análisis de proyecto son examinados y evaluados por una persona responsable, que determina sin son, o no son razonables.

En la revisión de los proyectos también ha sido verificado que existe alguna persona responsable de evaluar si con la solución propuesta se llegará a solventar el problema.

Otro de los puntos revisados de forma satisfactoria es que existe un proceso definido que se utiliza para encontrar una solución al problema propuesto.

Se ha comprobado que las necesidades de los usuarios son correctamente archivadas y firmadas por una persona responsable, junto con su aceptación, no – aceptación, motivos, etc.

Se ha comprobado que los requerimientos de control del proyecto han sido correctamente especificados.

Figura 81. Contestaciones correctas.

Si por el contrario el usuario administrador selecciona la respuesta “No correcto”, se mostrará la información elaborada a partir de las cuestiones que no han sido contestadas de forma satisfactoria.

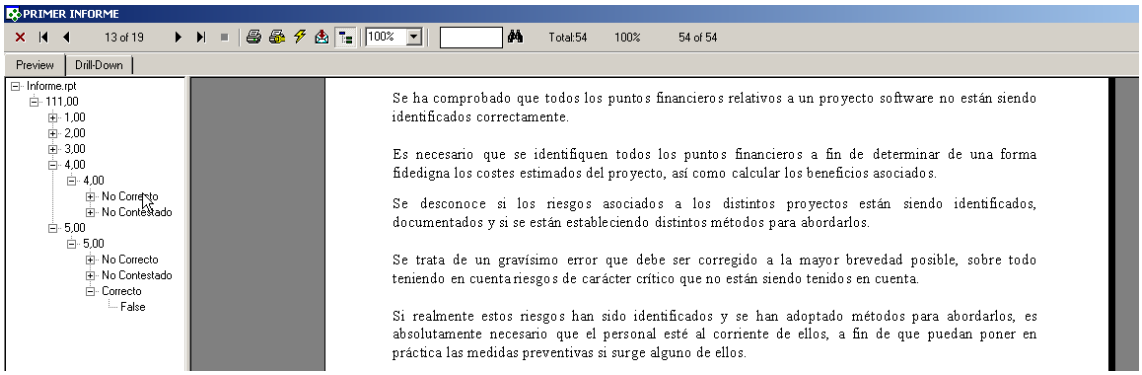


Figura 82. Contestaciones incorrectas.

En el ejemplo mostrado en la imagen anterior se ha seleccionado la información elaborada a partir de preguntas del cuestionario 4 que se han contestado de forma indebida.

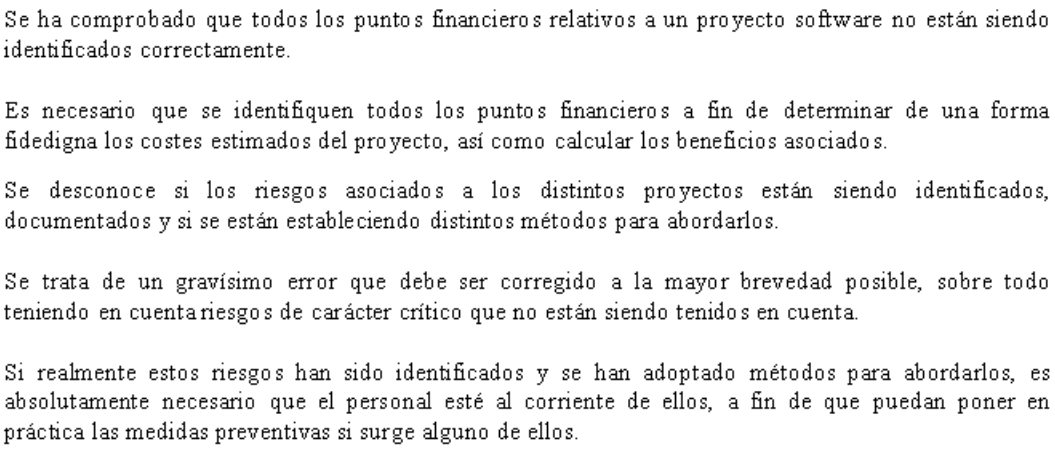


Figura 83. Ampliación contestaciones incorrectas.

Si por el contrario el usuario administrador selecciona la opción “no contestado”, se muestra la información elaborada a partir de preguntas del cuestionario cuya respuesta ha sido “no sabe / no contesta”.

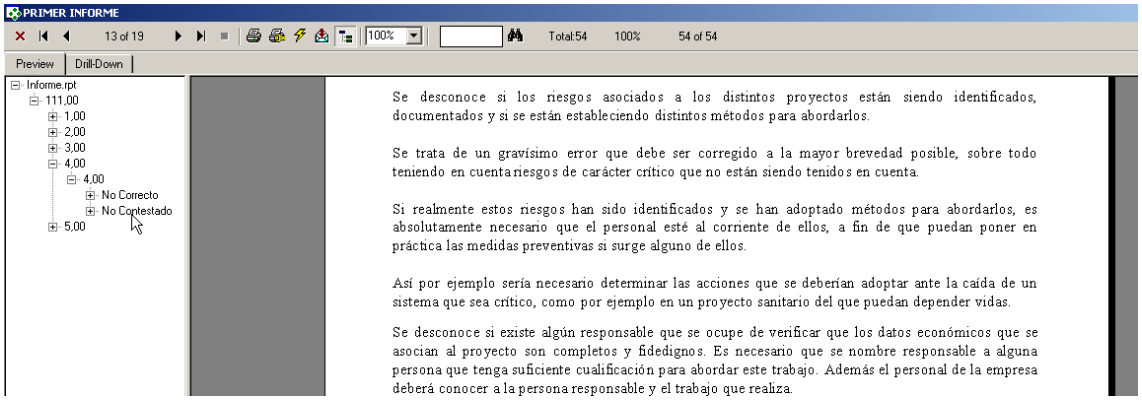


Figura 84. Contestaciones no contestadas.

Como puede observarse en la siguiente imagen el texto siempre se adapta conforme a la evaluación de las respuestas:

Se desconoce si los riesgos asociados a los distintos proyectos están siendo identificados, documentados y si se están estableciendo distintos métodos para abordarlos.

Se trata de un gravísimo error que debe ser corregido a la mayor brevedad posible, sobre todo teniendo en cuenta riesgos de carácter crítico que no están siendo tenidos en cuenta.

Si realmente estos riesgos han sido identificados y se han adoptado métodos para abordarlos, es absolutamente necesario que el personal esté al corriente de ellos, a fin de que puedan poner en práctica las medidas preventivas si surge alguno de ellos.

Así por ejemplo sería necesario determinar las acciones que se deberían adoptar ante la caída de un sistema que sea crítico, como por ejemplo en un proyecto sanitario del que puedan depender vidas.

Se desconoce si existe algún responsable que se ocupe de verificar que los datos económicos que se asocian al proyecto son completos y fidedignos. Es necesario que se nombre responsable a alguna persona que tenga suficiente cualificación para abordar este trabajo. Además el personal de la empresa deberá conocer a la persona responsable y el trabajo que realiza.

Se deberá tener en cuenta este punto, dado que al presupuestar un proyecto una de las variantes que se está teniendo en cuenta son los costes asociados al proyecto. Si estos están mal calculados es posible que la facturación no se realice de forma correcta y que posteriormente los gastos se disparen, perjudicando a la compañía.

Figura 85. Ampliación contestaciones no contestadas.

Como puede observarse todo el informe considera la evaluación realizada conforme a las respuestas de la fase de procesamiento.

A continuación se añade un pequeño ejemplo donde se muestra cómo varía la información del informe conforme a la respuesta presentada por el usuario, a fin que el mecanismo de generación de informes quede completamente claro.

Para el ejemplo un empleado accede con su usuario y su contraseña y responde a la pregunta 3 del cuestionario 6: ¿la documentación de análisis es adecuada y resulta conforme a los estándares?

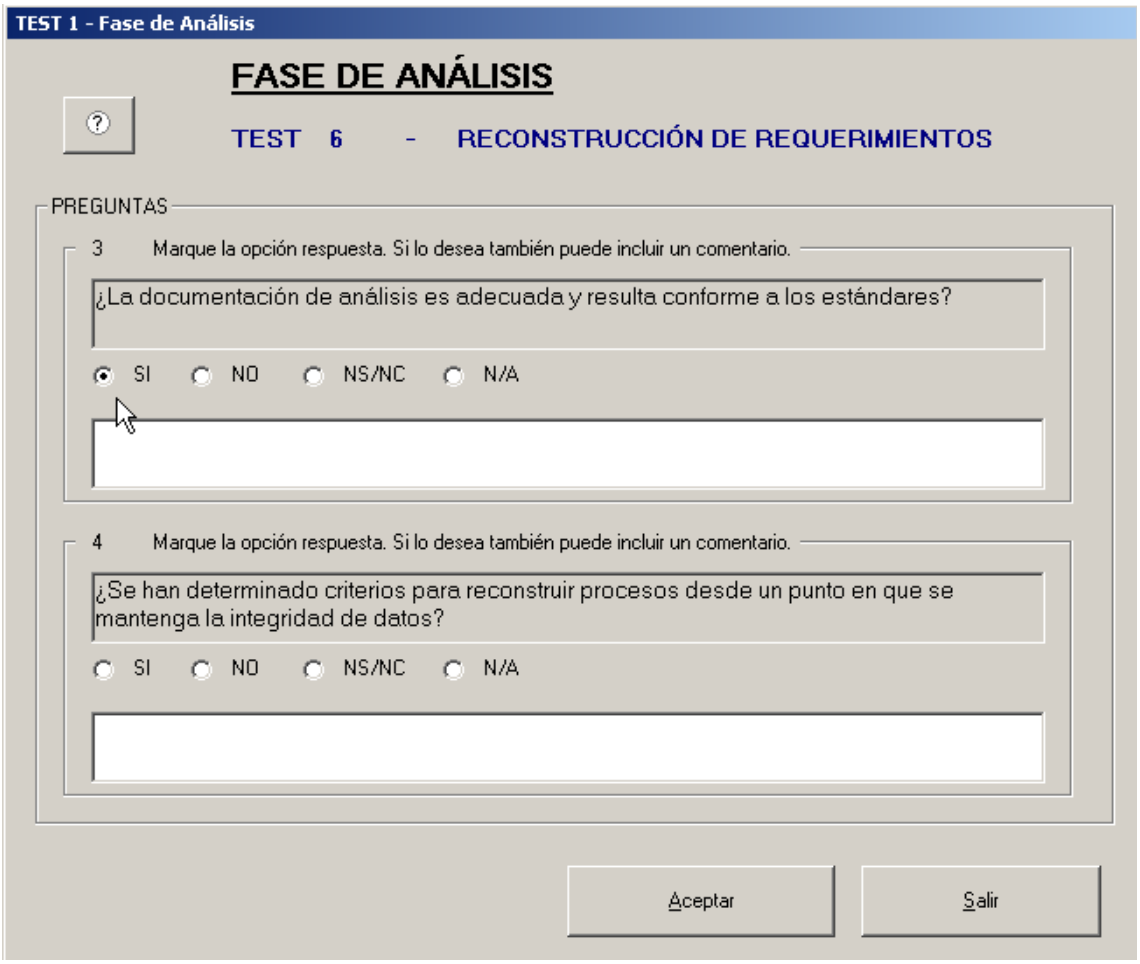


Figura 86. Pregunta 3 cuestionario 6.

Aprovechando que Audit Systems es concurrente e imaginando que el usuario administrador conoce que se están respondiendo nuevas preguntas, se va a proceder a actualizar la información del informe. Para ello se deberá hacer clic sobre el icono de refresco.

Figura 87. Refresco de datos.

Al hacerlo automáticamente el informe se actualizará con la nueva información introducida por el empleado.

A fin de localizar esta información de forma sencilla, dado el ejemplo que nos ocupa, utilizaremos el buscador de los informes. Probamos por ejemplo con la palabra documentación, dado la pregunta que nos ocupa.

Figura 88. Buscador.

Se introducirá la palabra al completo y se hará clic en el icono "Buscar". Al hacerlo la búsqueda nos irá situando en el contenido del informe que contenga la palabra seleccionada.

Si no se corresponde con la información que se está buscando bastará con hacer clic en el mismo icono de búsqueda para que busque la siguiente frase que contiene la palabra que se está buscando.

De esta forma se acabará encontrando la información que se busca:

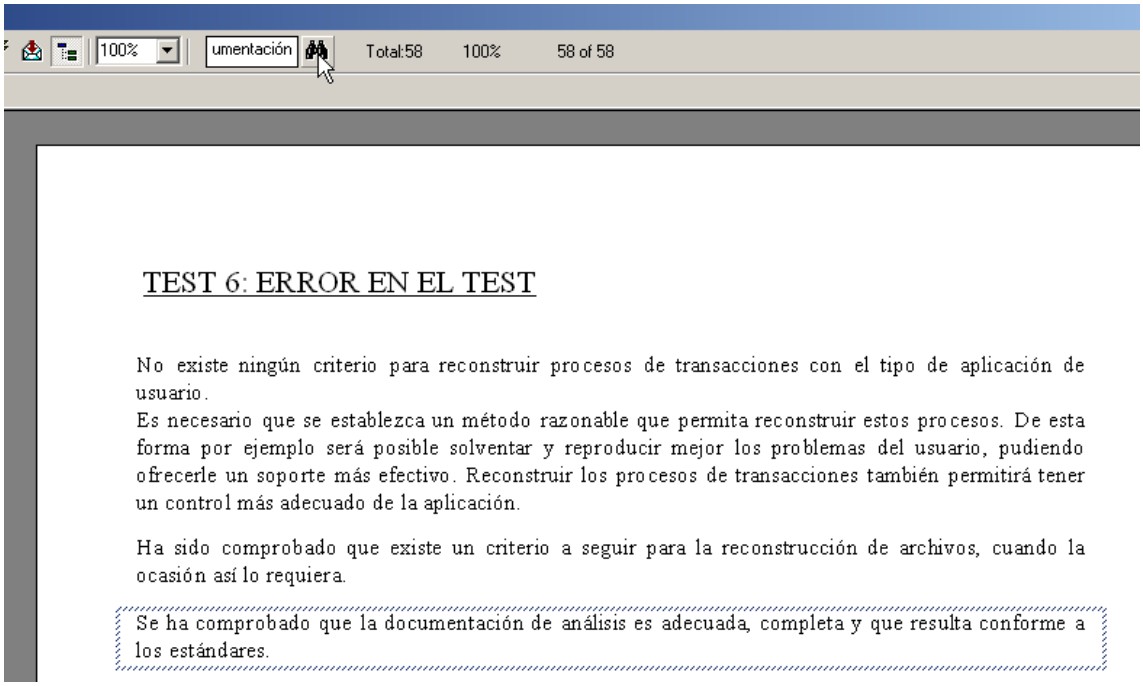


Figura 89. Cómo buscar.

Recuérdese que se preguntó si la documentación de análisis es adecuada y resulta conforme a los estándares; y que la respuesta fue que sí.

Por tanto la información que se muestra en el informe es: "Se ha comprobado que la documentación de análisis es adecuada, completa y que resulta conforme a los estándares".

Si se observan los puntos resúmenes correspondientes al final del cuestionario 6, se comprueba que no aparece información relacionada con esta pregunta.

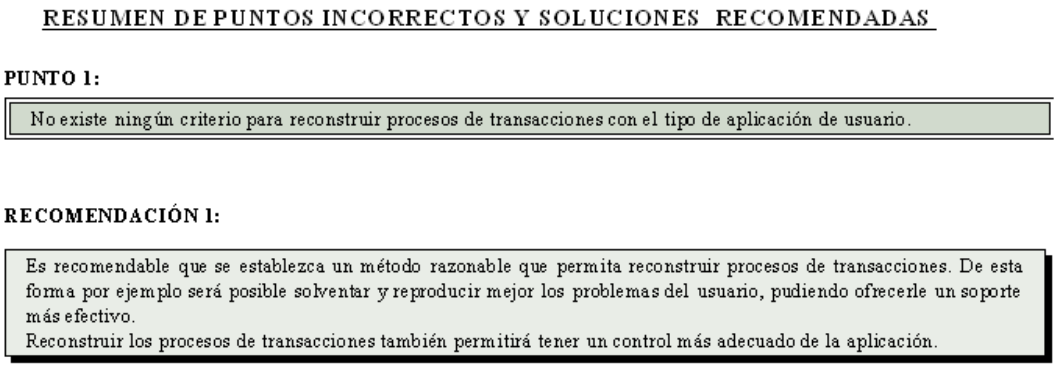


Figura 90. Información no encontrada en puntos resumen.

Continuando con el mismo ejemplo a continuación se detalla lo que ocurre si el empleado hubiese respondido de otra forma a la misma pregunta:

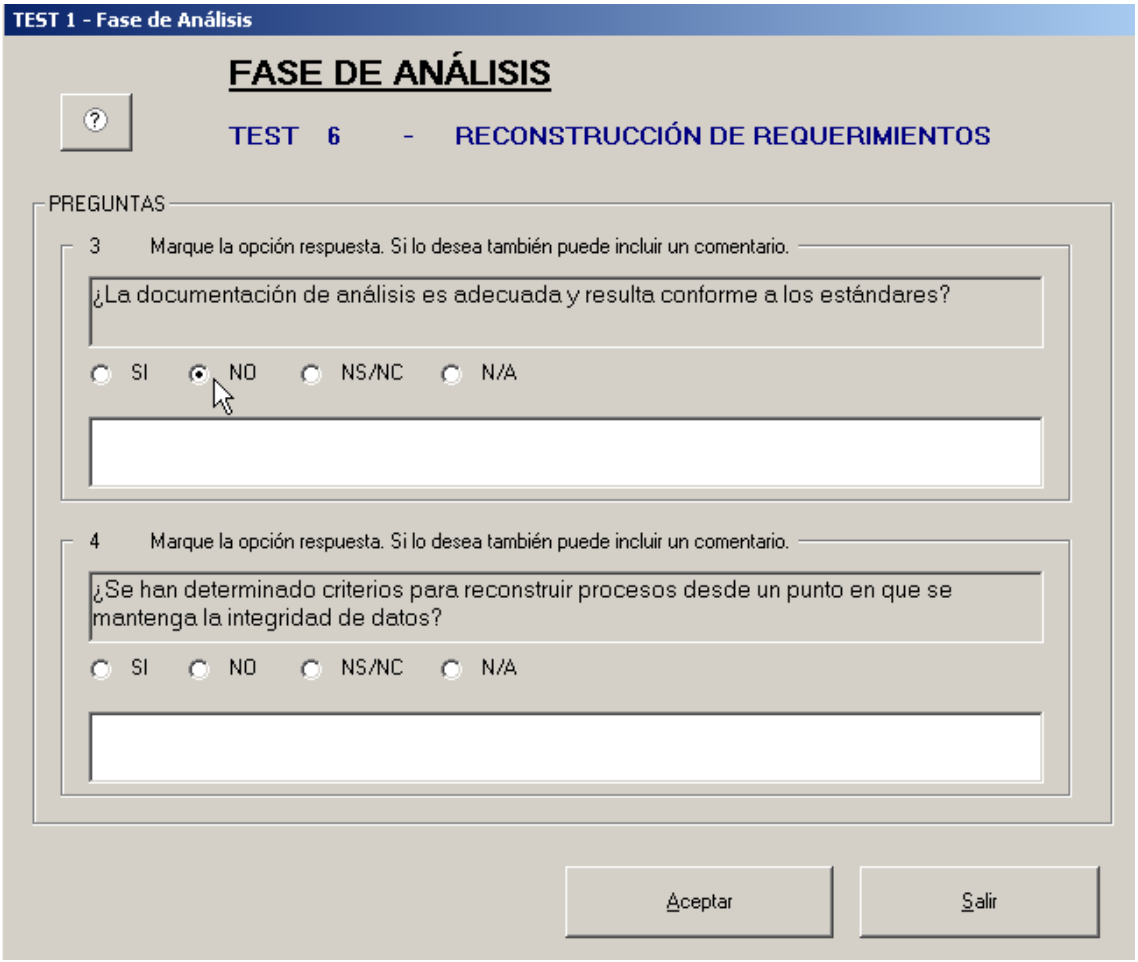
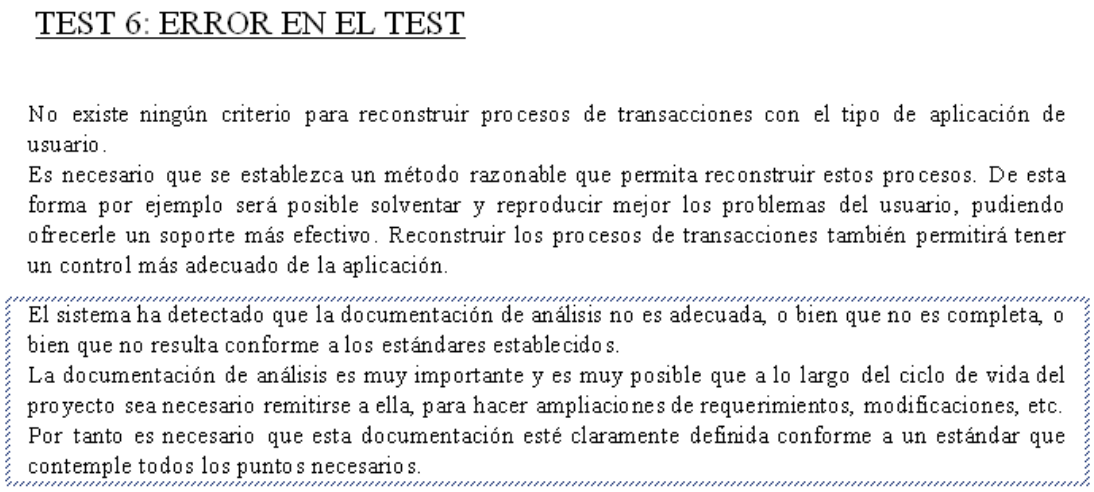


Figura 91. Opción 3 del cuestionario 6 negado.

De nuevo se refresca la información del informe para que lea las nuevas respuestas y se realiza la misma búsqueda.



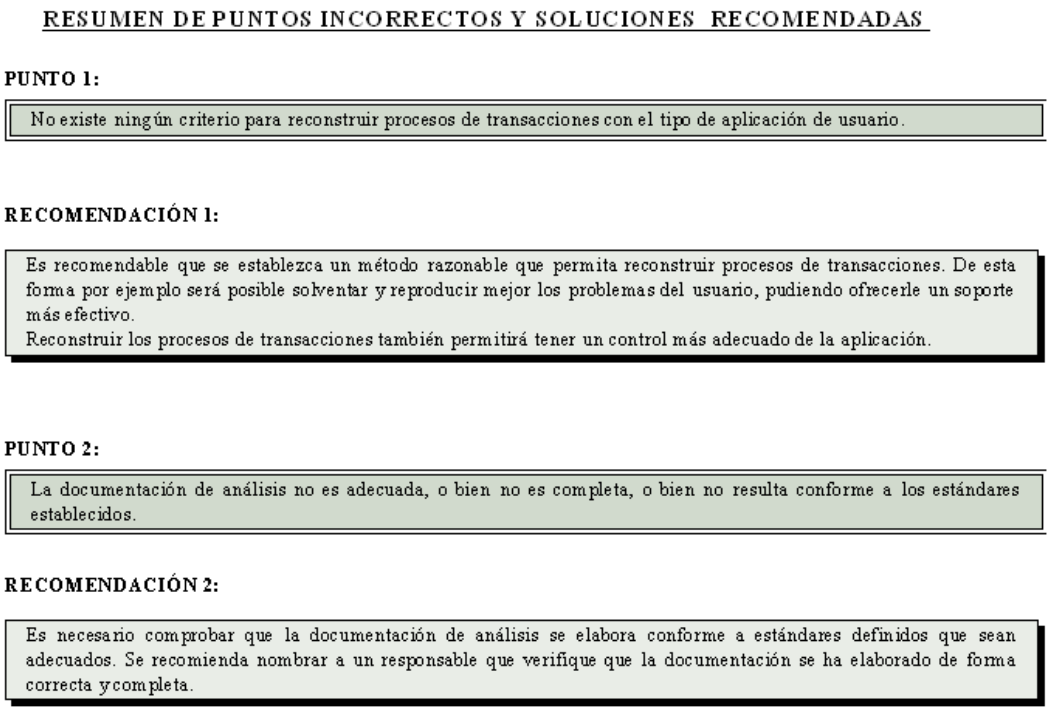
TEST 6: ERROR EN EL TEST

No existe ningún criterio para reconstruir procesos de transacciones con el tipo de aplicación de usuario.
Es necesario que se establezca un método razonable que permita reconstruir estos procesos. De esta forma por ejemplo será posible solventar y reproducir mejor los problemas del usuario, pudiendo ofrecerle un soporte más efectivo. Reconstruir los procesos de transacciones también permitirá tener un control más adecuado de la aplicación.

El sistema ha detectado que la documentación de análisis no es adecuada, o bien que no es completa, o bien que no resulta conforme a los estándares establecidos.
La documentación de análisis es muy importante y es muy posible que a lo largo del ciclo de vida del proyecto sea necesario remitirse a ella, para hacer ampliaciones de requerimientos, modificaciones, etc. Por tanto es necesario que esta documentación esté claramente definida conforme a un estándar que contemple todos los puntos necesarios.

Figura 92. Comparativa de respuesta.

Como puede comprobarse el texto que se muestra en el informe generado ha variado. Al contestar en el cuestionario que la documentación de análisis no es adecuada, el informe automáticamente genera esta nueva información, donde además de reseñar que no es adecuada se explica la importancia de la documentación de la fase de análisis.



RESUMEN DE PUNTOS INCORRECTOS Y SOLUCIONES RECOMENDADAS

PUNTO 1:

No existe ningún criterio para reconstruir procesos de transacciones con el tipo de aplicación de usuario.

RECOMENDACIÓN 1:

Es recomendable que se establezca un método razonable que permita reconstruir procesos de transacciones. De esta forma por ejemplo será posible solventar y reproducir mejor los problemas del usuario, pudiendo ofrecerle un soporte más efectivo.
Reconstruir los procesos de transacciones también permitirá tener un control más adecuado de la aplicación.

PUNTO 2:

La documentación de análisis no es adecuada, o bien no es completa, o bien no resulta conforme a los estándares establecidos.

RECOMENDACIÓN 2:

Es necesario comprobar que la documentación de análisis se elabora conforme a estándares definidos que sean adecuados. Se recomienda nombrar a un responsable que verifique que la documentación se ha elaborado de forma correcta y completa.

Figura 93. Información añadida en el resumen.

Nótese también en el resumen final del capítulo como se ha detectado esta incorrección y ahora aparece un nuevo punto, el punto 2, donde se resume que la documentación de análisis no es adecuada o bien no resulta conforme a los estándares.

Y véase también la nueva recomendación que se ha generado para este punto: "es necesario comprobar que la documentación de análisis se elabora conforme a estándares definidos que sean adecuados. Se recomienda nombrar a un responsable que verifique que la documentación se ha elaborado de forma correcta y completa."

Por último se comprobará con el mismo ejemplo qué sucede si el empleado hubiese contestado con la opción de la aplicación "no sabe / no contesta".

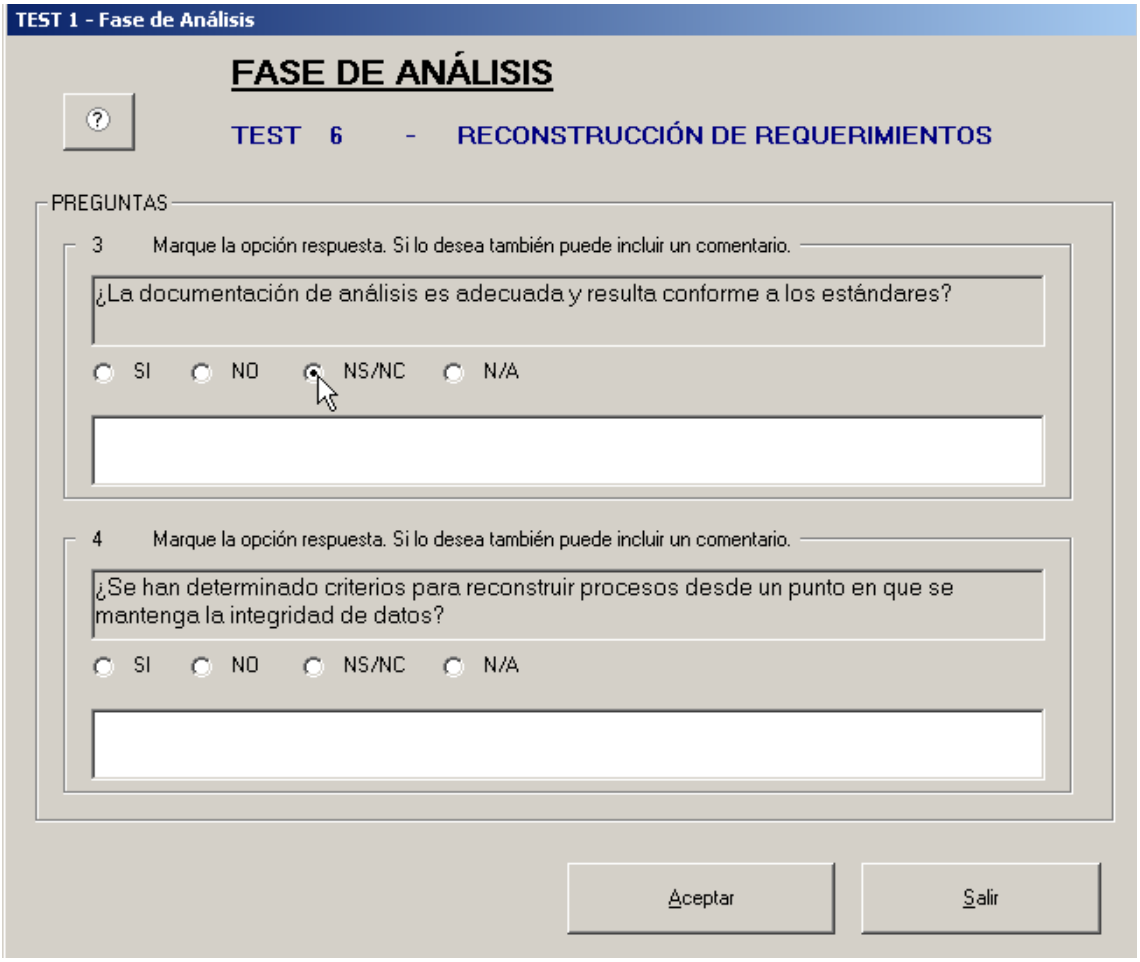


Figura 94. Respuesta No sabe, no contesta.

Al realizar la misma operación de refresco y de búsqueda, se comprueba que los textos anteriores han variado.

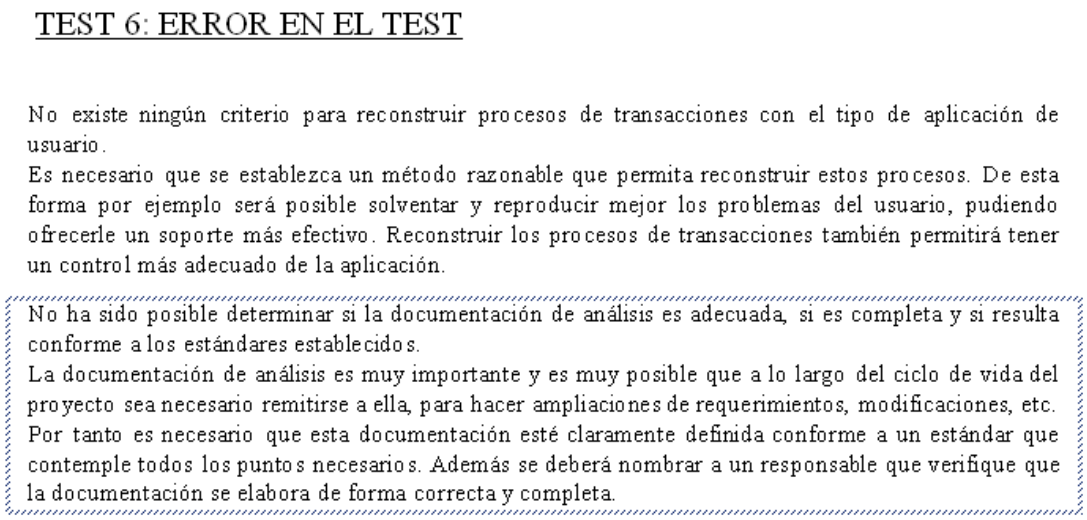


Figura 95. Información con respuesta No sabe, no contesta.

Para el nuevo caso se explica que no ha sido posible determinar si la documentación de análisis es adecuada, si es completa y si resulta conforme a los estándares establecidos.

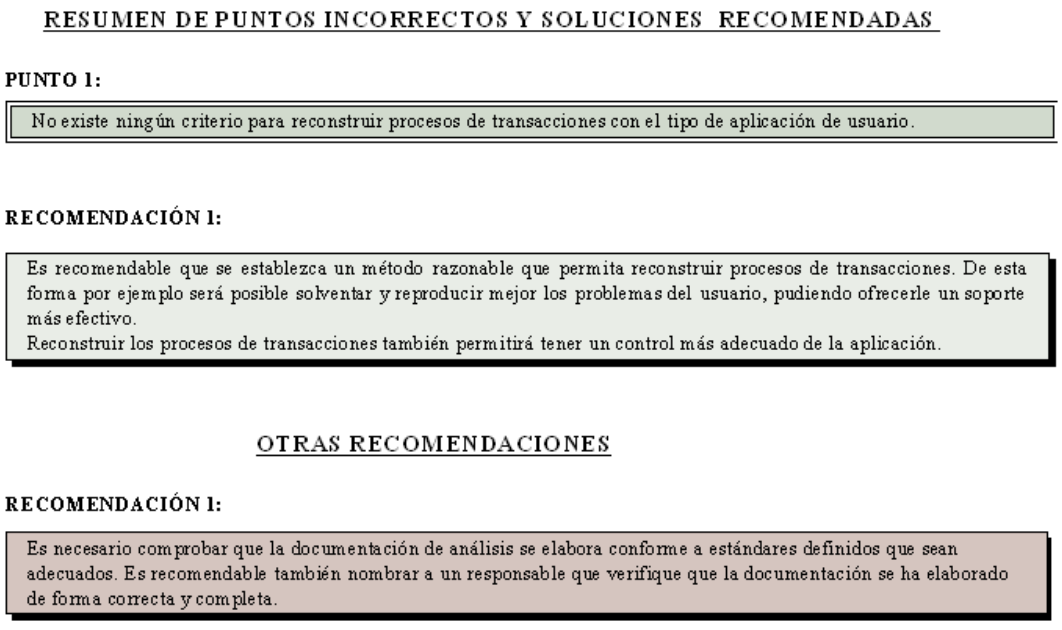


Figura 96. Nueva recomendación.

Como puede observarse en los puntos resúmenes a tener en cuenta del final del capítulo, no se ha generado un nuevo punto incorrecto, si no una única recomendación: "es necesario comprobar que la documentación de análisis se elabora conforme a estándares definidos que sean adecuados…"

Resulta fascinante el modo en que Audit Systems evalúa las respuestas conforme a la metodología que contiene y es capaz de generar informes finales con capítulos, textos orientados, puntos a corregir y recomendaciones a seguir.

Como se explicó con anterioridad, una vez generado el informe de auditoría es importante que el auditor experto tenga accesible la información y que pueda editar su contenido. De esta forma si ha averiguado nueva información, si quiere editar algún punto, añadir alguna nueva referencia, etc., podrá realizarlo.

Para ello se podrá usar la funcionalidad de exportación de informe a distintos formatos.

Figura 97. Exportar informe.

Esta funcionalidad permite exportar el informe generado a distintos formatos, en función de las aplicaciones que tenga instalado el equipo que se esté usando. A continuación se verá un ejemplo de exportación del informe a formato Word.

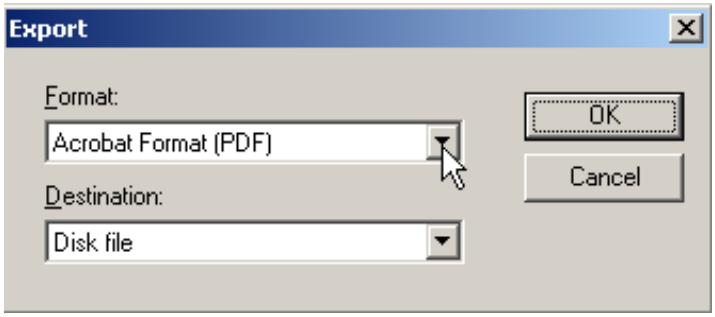


Figura 98. Ventana de exportación.

Al hacer clic sobre el icono de exportación se muestra la ventana anterior. Entonces se deberá desplegar el selector de formato para seleccionar el formato al cual se desea exportar el informe.

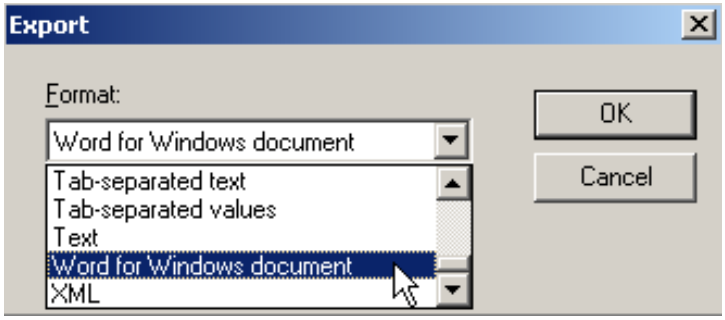


Figura 99. Selector de formato.

Una vez seleccionado el formato de exportación del informe, se seleccionará la unidad de destino.

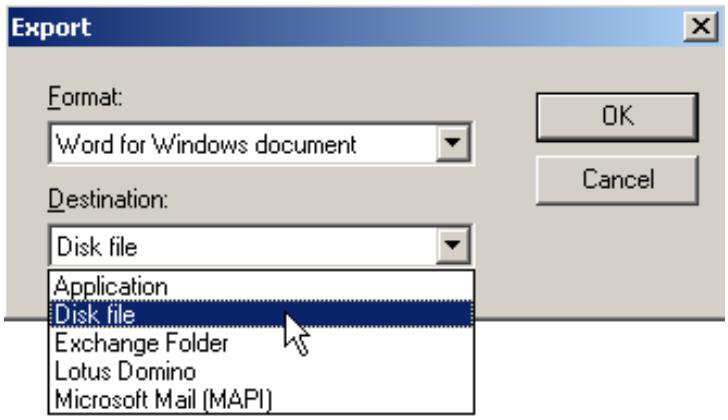


Figura 100. Selector de destino.

En esta ocasión se selecciona como destino el disco duro del ordenador. Se hará clic en el botón aceptar.

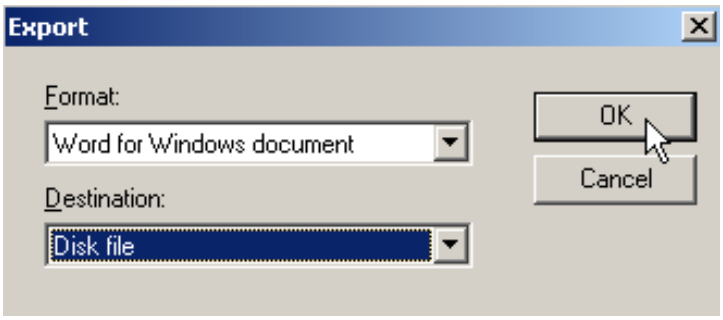


Figura 101. Comenzar la exportación.

A continuación una ventana nos permitirá introducir el nombre con que se desea exportar el archivo y seleccionar el directorio donde se quiere guardar la exportación.

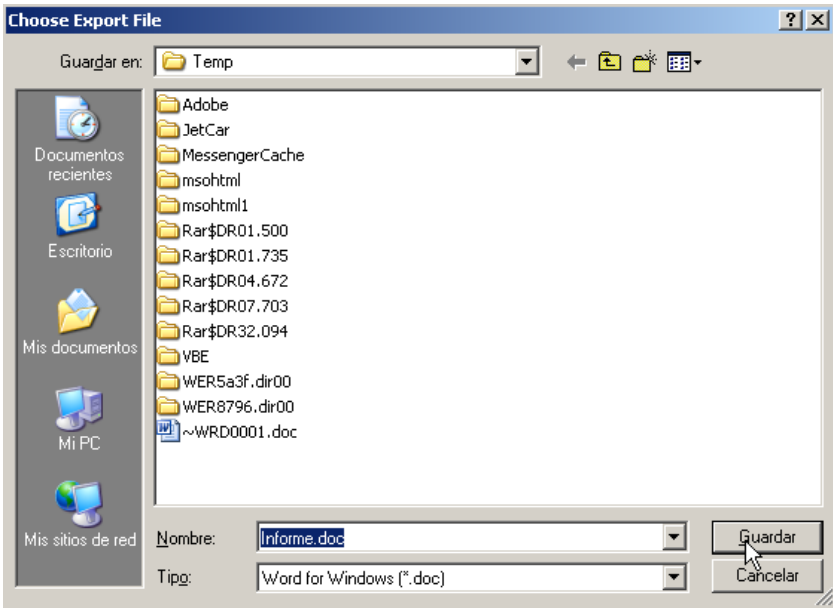


Figura 102. Seleccionar destino.

Es necesario tener en cuenta que las ediciones que se realicen en el fichero exportado no se actualizarán en el informe general de la aplicación. Téngase en cuenta que el administrador podrá realizar tantas exportaciones como quiera utilizando los formatos que desee.

Por ello se aconseja al auditor experto no exportar el informe hasta que todas las respuestas de los cuestionarios hayan sido contestadas y se disponga del informe final.

Una vez finalizado el proceso de respuestas a los cuestionarios y generado el informe final, se podrá proceder a su guardado en cualquier formato y edición si procede; y se podrán usar las opciones de impresión para imprimir el informe.

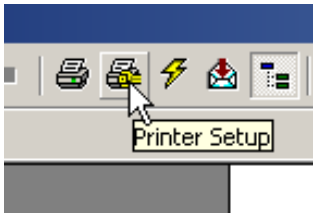


Figura 103. Configurar impresora.

Este icono permite configurar la impresora y seleccionar la impresora por la que se desea imprimir.

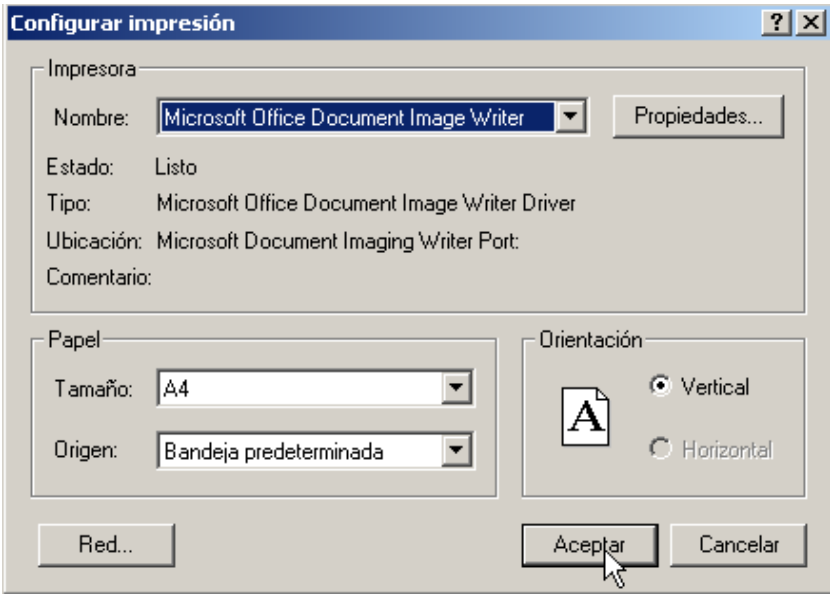


Figura 104. Ventana de configuración de impresora.

El icono contiguo permite imprimir.

Figura 105. Imprimir.

Al seleccionarlo se mostrará la siguiente ventana, donde se puede seleccionar si se quiere imprimir todo, un rango de hojas determinado –desde, hasta-; y también qué número de copias se quieren imprimir.

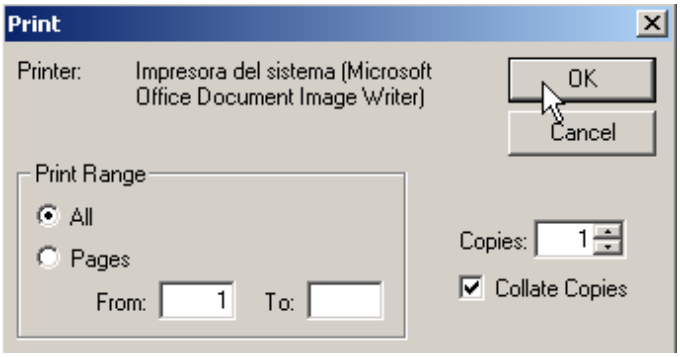


Figura 106. Selecciones de impresión.

Una vez finalizado el trabajo con los informes se hará clic en el icono salir.

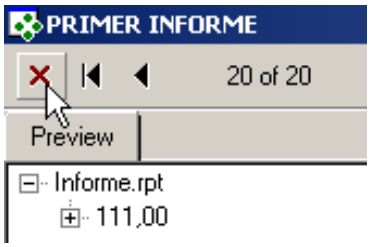


Figura 107. Salir informes.

4. CONCLUSIONES.

A lo largo de este documento se ha constatado que Audit Systems es una aplicación de gran ayuda en las gestiones de auditoría, tan necesarias en los momentos actuales. Sin duda alguna Audit Systems permitirá ahorrar tiempo en el proceso, permitiendo de este modo una realización de auditorías a un menor coste para las empresas; y un mayor margen de beneficio a las empresas auditoras.

Naturalmente Audit Systems puede ser complementada con nuevos módulos en función de las necesidades de cada momento. Su construcción modular lo permite. Así por ejemplo sería posible añadir un módulo de seguridad para revisión automática de puertos, accesos, passwords, etc.

Sin necesidad de nuevas extensiones de la aplicación, uno de los valores más interesantes de Audit Systems es que permite la actualización de las normativas vigentes. Gracias a ello se dispone de una aplicación capaz de evaluar los procesos de información y de generar informes que además nunca quedará desfasada.

Indirectamente también se ha conseguido un sistema de almacenaje y evaluación periódica, dado que Audit Systems recoge datos de las empresas, fruto del análisis de la auditoría y los almacena, por lo que podrán ser revisados y comparados a fin de determinar una evolución satisfactoria de los procesos.

Ha sido un éxito el diseño de los informes, la ordenación automática de la información, las recomendaciones y sugerencias que se generan automáticamente en los capítulos finales… Se puede concluir por tanto que se ha logrado el objetivo que se perseguía y que gracias a Audit Systems se podrán simplificar en gran medida los procesos de Auditoría.

5. PRESUPUESTO

5.1. PLANIFICACIÓN DEL PROYECTO.

	Nombre de tarea	Duración	Comienzo	Fin
1				
2	**AUDIT SYSTEMS**	0 días	dom 28/11/10	dom 28/11/10
3				
4	Análisis normativas, cuestionarios y BBDD	90 días	mar 28/04/09	lun 31/08/09
5	Análisis y diseño	90 días	mar 01/09/09	lun 04/01/10
6	Desarrollo y depuración	150 días	mar 05/01/10	lun 02/08/10
7	Informes y conexiones BBDD	60 días	mar 03/08/10	lun 25/10/10
8	Documentación	30 días	mar 26/10/10	lun 06/12/10
9	Presentación	1 día	mar 07/12/10	mar 07/12/10
10	Entrega	0 días	mar 07/12/10	mar 07/12/10

Figura 108. Hitos Planificación.

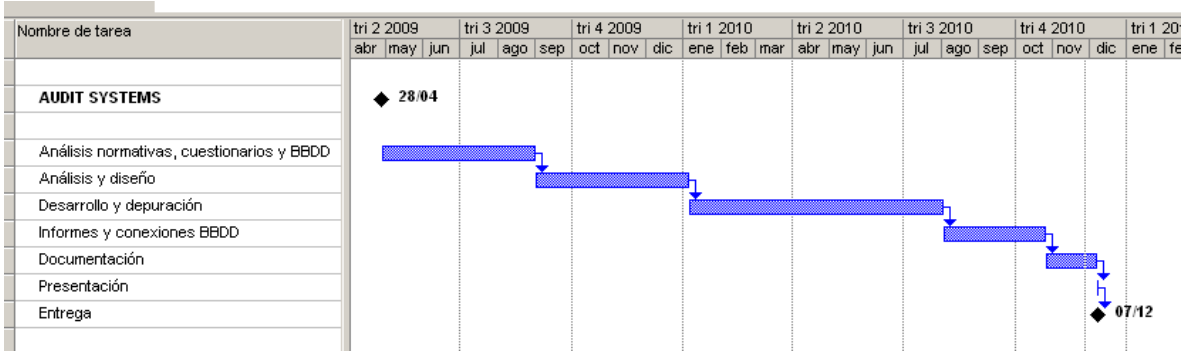


Figura 109. Planificación temporal.

5.2. PRESUPUESTO POR PARTIDAS.

MANO DE OBRA	UNIDAD	CANT	PRECIO	IMPORTE
Normativa, cuestionarios y bases de datos	mes	3,00	2.000,00	6.000,00
Análisis y diseño	mes	3,00	2.000,00	6.000,00
Desarrollo y depuración	mes	5,00	2.000,00	10.000,00
Informes y conexiones de bases de datos	mes	2,00	2.000,00	4.000,00
Documentación	mes	1,00	2.000,00	2.000,00
TOTAL MANO DE OBRA				28.000,00

MEDIOS MATERIALES	UNIDAD	CANT	PRECIO	IMPORTE
Ordenador portátil	ud	1,00	529,00	529,00
Microsoft Office 2010 (Versión hogar y pequeña empresa)	ud	1,00	379,00	379,00
Microsoft Visual Studio 2008 (Professional Edition)	ud	1,00	550,00	550,00
Microsoft SQL 2008 (Standard Edition)	ud	1,00	1.300,00	1.300,00
Cystal Reports (Professional Edition)	ud	1,00	354,00	354,00
TOTAL MEDIOS MATERIALES				3.112,00

VARIOS	UNIDAD	CANT	PRECIO	IMPORTE
Transporte y desplazamientos	varios	1,00	150,00	150,00
Fotocopias y encuadernación	ud	1,00	200,00	200,00
TOTAL VARIOS				350,00

TOTAL PRESUPUESTO	31.462,00

El presupuesto total de este proyecto asciende a la cantidad de **31.462 EUROS**.

El ingeniero proyectista:

Mª Isabel López García
En Leganés a 18 de Octubre de 2010

5.3. PRESUPUESTO DE VENTA MEDIANA EMPRESA.

AUDIT SYSTEMS	UNIDAD	CANT	IMPORTE
Licencias de Uso	Ud	80	25.000
Formación Aplicativo	Días	3	1.500
Formación Actualización Normativas	Días	2	1.000
TOTAL			27.500,00

MATERIAL	UNIDAD	CANT	PRECIO	IMPORTE
Ordenador servidor de datos	Ud	2,00	800,00	1.600
Microsoft SQL 2008 (Standard Edition)	Ud	1,00	1.300,00	1.300
Cystal Reports (Professional Edition)	Ud	1,00	354,00	354
TOTAL MEDIOS MATERIALES				3.254,00

VARIOS	UNIDAD	CANT	PRECIO	IMPORTE
Transporte y desplazamientos	Varios			250
Comidas	Ud	1,00	200,00	100
TOTAL VARIOS				350,00

TOTAL PRESUPUESTO	31.104,00

El presupuesto total de este proyecto asciende a la cantidad de **31.104 EUROS**.

El ingeniero proyectista:

Mª Isabel López García
En Leganés a 18 de Octubre de 2010

6. GLOSARIO

COBIT	Control Objectives for Information and related Technology
ISACA	Information Systems Audit and Control Association
MARION	Método Cuantitativo de Análisis de Riesgos perteneciente al grupo de Metodologías de Evaluación de Sistemas.
SEDISI	Asociación Española de Empresas de Tecnologías de la Información
ISO	International Organization for Standardization

7. REFERENCIAS

[.NET] *Microsoft .NET*. Microsoft Corporation. 2002. Disponible [Internet]: <http://www.microsoft.com/net> [28 de febrero de 2011]

[BC96] Bernal Montañés, R. y Coltell O. 'Auditoría de los Sistemas de Información', Servicio de Publicaciones de la Universidad Politécnica de Valencia, 1996

[Dia05] Díaz Palacios, J. 'Documento de Seguridad para la gestión de archivos que contienen datos de carácter personal', biblioteca UC3M (EPS), 2005

[MR94] Morant Ramón, J. Luis, y Ribagorda Garnacho, A.'Seguridad y Protección de la Información', Editorial Universitaria Ramón Areces, 1994

[Pes02] Peso Navarro, Emilio del 'La Seguridad de los Datos de Carácter Personal', Editorial Díaz de Santos, biblioteca UC3M (EPS), 2002

[Pes01] Peso Navarro, Emilio del 'Peritajes Informáticos', Editorial Díaz de Santos, biblioteca UC3M (EPS), 2001

[PP08] PiattiniVelthuis, Mario G. y Peso Navarro, Emilio del 'Auditoría de Tecnologías y Sistemas de Información', Editorial RA-MA, biblioteca UC3M (EPS), 2008

[RAE93] Real Academia de la Lengua Española. *Diccionario de la Lengua Española*. Edición 21ª. 1993. ISBN: 84-239-6813-8. Disponible [Internet]: <http://www.rae.es> [28 de febrero de 2011]

[Ram07] Ramírez Sánchez, R 'La auditoría informática y la generación de informes', biblioteca UC3M (EPS), 2007.

[Rib96] Ribagorda Garnacho, A. 'Seguridad de las Tecnologías de la Información, en Ámbito Jurídico de las Tecnologías de la Información', Consejo General del Poder Judicial, 1996

[Rib00] Ribagorda Garnacho, A. 'Seguridad de las Transacciones Electrónicas II', Aranzadi, 2000

[Rib99] Ribagorda Garnacho, A. 'Informática para la Empresa y Técnicas de Programación', Centro de Estudios Ramón Areces, 1999

[Rib97] Ribagorda Garnacho, A. 'Glosario de Términos de las TI', Ediciones Coda, 1997

[Rib04] Ribagorda Garnacho, A. 'Avances en Criptología y en Ciencias de la Información', Ediciones Díaz Santos, SA, 2004

[Vic05] Vicente Cabrerizo, Miguel de 'Auditoría del desarrollo de proyectos informáticos', PFC Escuela Politécnica, 2005